EXHIBIT A

skip to main content

Print

CASE INFORMATION

CV-20-932778 DANIEL BOZIN, ET AL. vs. DELOITTE CONSULTING LLP

Docket Information

Filing Date	Docket Party	Docket Type	Docket Description	View Image
05/28/2020	P	MO	MOTION FOR TEMPORARY RESTRAINING ORDER...PLAINTIFF(S) DANIEL BOZIN(P1), TIMOTHY SMITH(P2) and ALEXANDRIA POLICHENA(P3). PLAINTIFFS EMERGENCY MOTION PURSUANT TO CIV. R. 65 FOR A TEMPORARY RESTRAINING ORDER AND OR PRELIMINARY INJUNCTION	
05/28/2020	P1	SF	DEPOSIT AMOUNT PAID MARC E DANN	
05/28/2020	P1	CO	AMENDED COMPLAINT $75 FIRST AMENDED CLASS ACTION COMPLAINT FOR DAMAGES	
05/21/2020	N/A	SF	JUDGE DAVID T MATIA ASSIGNED (RANDOM)	
05/21/2020	P1	SF	LEGAL RESEARCH	
05/21/2020	P1	SF	LEGAL NEWS	
05/21/2020	P1	SF	LEGAL AID	
05/21/2020	P1	SF	COURT SPECIAL PROJECTS FUND	
05/21/2020	P1	SF	COMPUTER FEE	
05/21/2020	P1	SF	CLERK'S FEE	
05/21/2020	P1	SF	DEPOSIT AMOUNT PAID MARC E DANN	
05/21/2020	N/A	SF	CASE FILED: COMPLAINT, SERVICE REQUEST	

Only the official court records available from the Cuyahoga County Clerk of Courts, available in person, should be relied upon as accurate and current.
Website Questions or Comments.

NAILAH K. BYRD
CUYAHOGA COUNTY CLERK OF COURTS
1200 Ontario Street
Cleveland, Ohio 44113

Court of Common Pleas

New Case Electronically Filed: COMPLAINT
May 21, 2020 13:04

By: MARC E. DANN 0039425

Confirmation Nbr. 2001679

DANIEL BOZIN, ET AL.

vs.

DELOITTE CONSULTING LLP

CV 20 932778

Judge: DAVID T. MATIA

Pages Filed: 21

IN THE COURT OF COMMON PLEAS
CUYAHOGA COUNTY, OHIO

DANIEL BOZIN, individually and on behalf of all others similarly situated, % DannLaw PO Box 6031040 Cleveland, OH 44103 AND TIMOTHY SMITH, individually and on behalf of all others similarly situated, % DannLaw PO Box 6031040 Cleveland, OH 44103 AND ALEXANDRIA POLICHENA, individually and on behalf of all others similarly situated, % DannLaw PO Box 6031040 Cleveland, OH 44103 Plaintiffs, v. DELOITTE CONSULTING LLP % Corporation Service Company 50 West Broad Street, Suite 1330 Columbus, OH 43215 Defendant.	Case No.: Judge **CLASS ACTION COMPLAINT FOR DAMAGES** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs DANIEL BOZIN ("Bozin"), TIMOTHY SMITH ("SMITH"), and ALEXANDRIA POLICHENA ("Polichena")("Plaintiffs"), by and through their attorneys, bring this class action lawsuit on behalf of themselves and all other persons similarly situated, and for their Class Action Complaint against Defendant DELOITTE CONSULTING LLP ("Deloitte" or

Electronically Filed 05/21/2020 13:04 / / CV 20 932778 / Confirmation Nbr. 2001679 / CLLMD

"Defendant"), Plaintiffs allege with personal knowledge with respect to themselves individually and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters, as follows:

PARTIES

1. Plaintiff DANIEL BOZIN is a natural person with a principal place of residence located in Cuyahoga County, Ohio.

2. Plaintiff TIMOTHY SMITH is a natural person with a principal place of residence in Franklin County, Ohio.

3. Plaintiff ALEXANDRIA POLICHENA is a natural person with a principal place of residence in Portage County, Ohio.

4. Defendant DELOITTE CONSULTING LLP is a Delaware limited liability company with a principal place of business in Hermitage, TN.

5. Deloitte is a wholly-owned subsidiary of Deloitte LLP.

6. Venue lies in this Court pursuant to Civ. R. 3(B) as a substantial portion, if not all, of the events that form the basis of this Class Action Complaint occurred in Cuyahoga County, Ohio; Defendant conducted activity that gave rise to the claims for relief in this County; and Defendant maintains an office in this county.

THE DATA BREACH

7. Plaintiffs bring this suit on behalf of themselves and a Class of similarly situated individuals against Defendant for Defendant's failure to secure and protect Plaintiffs' and Class members' personal and financial information.

8. At one of the worst times in the lives of Plaintiffs and Class members, when they find themselves unemployed in the midst of a pandemic and resulting recession, Deloitte was

brought in as an expert consultant by the State of Ohio to expedite the processing of plaintiffs' and Class members' unemployment claims. However, Deloitte negligently and recklessly made the Plaintiffs' and Class members' path to recovery significantly harder by putting their identity and credit standing at risk.

9. On May 20, 2020, Deloitte sent Bozin an email, which is attached as Exhibit 1 to this Complaint (the "Notice").

10. In the Notice, Deloitte advised Bozin of the following:

> Dear PUA Applicant:
>
> Deloitte Consulting is currently under contract with the Ohio Department of Job and Family Services (ODJFS) to assist the state of Ohio in administering the Pandemic Unemployment Assistance (PUA) program. Deloitte discovered on May 15, 2020 that your name, Social Security number, and street address pertaining to your application for and receipt of unemployment compensation benefits inadvertently had the capability to be viewed by other unemployment claimants. Thereafter, Deloitte immediately began an investigation and upon discovering the exposure, Deloitte immediately took steps to stop further access to and exposure of your personal information.
>
> At this time, there is no evidence or indication to believe that your personal information was improperly used; therefore, our actions, as well as the actions you may want to consider, are preventative.
>
> As a precaution, you may want to monitor your credit by obtaining a copy of your credit report from one of the three national credit bureaus. Federal law entitles every individual to one free credit report per year from each of the three main bureaus.
>
> You may also have a fraud alert placed on your consumer credit file by contacting one of the national credit bureaus. Once one credit bureau places a fraud alert on your credit file, it notifies the other two bureaus. Fraud alerts are typically in effect for 90 days but can be renewed. The credit bureaus may be contacted at:

> Equifax: (800) 525-6285 (http://www.equifax.com)
> Experian: (888) 397-3742 (http://www.experian.com)
> TransUnion: (800) 680-7289 (http://www.tuc.com)
>
> Additionally, Ohio law allows you to place a security freeze on your credit report by contacting one of the bureaus listed above. Should you wish to open a new line of credit while your report is frozen, you may temporarily lift this security freeze by telephone or online by providing a security code. Credit reporting agencies may charge a fee of no more than $5 for each freeze and unfreeze of your report.
>
> If you wish to receive free Experian IdentityWorks identity protection services for the next 12 months, you will receive a follow-up email with enrollment details that will be sent to you via Deloitte or directly from Experian within 3-5 days.
>
> Finally, to find out more about protecting your personal information, visit the Ohio Attorney General's IdentityTheft protection page (http://www.ohioattorneygeneral.gov/IdentityTheft) and/or the Federal Trade Commission's identity theft assistance page (https://www.consumer.ftc.gov/features/feature-0014-identitytheft).
> We apologize for any concerns or inconvenience as a result of this unauthorized incident. Please be assured that we take very seriously our responsibility to safeguard the personal information you entrust to our care, and deeply regret that this incident occurred.
>
> If you have questions or concerns that remain unaddressed after reviewing this information, please email:
> DeloitteIdentityhelp@jfs.ohio.gov.

See Exhibit 1 at pp. 1-2.

11. On May 20, 2020, Deloitte sent the same Notice to Smith via e-mail.

12. On May 20, 2020, Deloitte sent the same Notice to Polichena via e-mail.

13. The Notice acknowledges that a treasure trove of highly sensitive personal information was subject to unauthorized access by foreign IP addresses, as well as other claimants for pandemic unemployment assistance (the "Data Breach"). *See* Exhibit 1 at p. 1

14. As a result of the Data Breach, Plaintiffs and Class members must now be vigilant and review their credit reports for suspected incidents of identity theft, and to educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft.

15. Data security breaches have dominated the headlines for the last two decades, and it does not take an IT industry expert to know that major businesses like Deloitte are at risk.

16. The general public can tell you the names of some of the biggest data breaches: LabCorp, Quest Diagnostics, Yahoo, Equifax, Marriott International, Target, Home Depot, Anthem, Heartland Payment Systems, and TJX Companies, Inc.[1]

17. Deloitte is no stranger to data breaches and phishing scams of its own employees.[2]

18. Upon information and belief, Deloitte failed to implement reasonable industry standards necessary to prevent a data breach, including the FTC's guidelines, resulting in the Data Breach.

19. Likewise, Deloitte failed to create, maintain, and/or comply with a written cybersecurity program that incorporated physical, technical, and administrative safeguards for the protection of personal information and reasonably conformed to an industry recognized cybersecurity framework, resulting in the Data Breach.

20. Because of its failure to create, maintain, and/or comply with a necessary cybersecurity program, Deloitte was unable to ensure the protection of information security and confidentiality, protect against obvious and readily foreseeable threats to information security and confidentiality or the unauthorized access of the PII, resulting in the Data Breach.

---

[1] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[2] *See, e.g.*, *Source: Deloitte Breach Affected All Company Email, Admin Accounts*, Krebsonsecurity.com (September 25, 2017) (last visited May 20, 2020) https://krebsonsecurity.com/2017/09/source-deloitte-breach-affected-all-company-email-admin-accounts/

DAMAGES FROM DATA BREACHES

21. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[3]

22. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[4]

23. Identity thieves use stolen personal information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

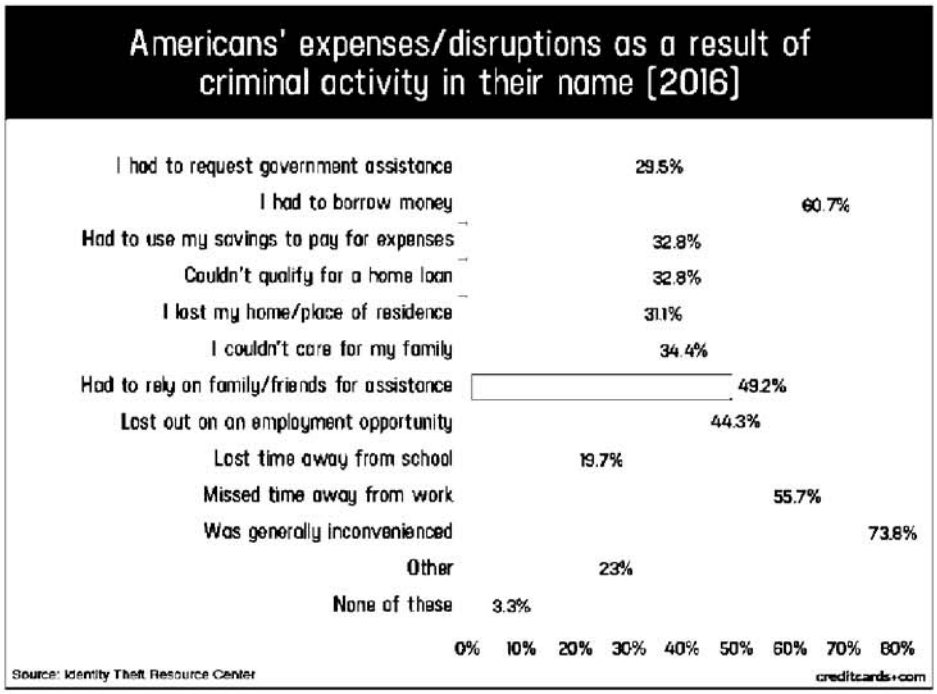
24. Identity thieves can also use SSNs to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and SSN to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

25. A study by the Identity Theft Resource Center show the multitude of harms caused by fraudulent use of personal and financial information:

---

[3] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," pg. 2, by U.S. Government Accountability Office, June 2007, at: https://www.gao.gov/new.items/d07737.pdf (last visited May 20, 2020) ("GAO Report").

[4] *See* https://www.identitytheft.gov/Steps (last visited May 20, 2020).



Source: "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/17, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited May 20, 2020).

26. There may be a time lag between when harm occurs versus when it is discovered, and also between when personal and financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

27. Personal and financial information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information

on the "cyber black-market" for years.

28. Thus, there is a strong probability that entire batches of stolen information have been dumped on the black market, and are yet to be dumped on the black market, meaning Plaintiffs and Class members are at an increased risk of fraud and identity theft for many years into the future.

29. Data breaches are preventable.[5] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[6] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[7]

30. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[8]

FACTS RELEVANT TO PLAINTIFF DANIEL BOZIN

31. Bozin is a citizen of Ohio (and was during the period of the Data Breach).

32. On May 13, 2020, Bozin applied online with the Ohio Department of Job and Family Services ("ODJFS") for pandemic unemployment assistance ("PUA").

33. At the time Bozin applied online for PUA, the website was being operated by Deloitte.

---

[5]Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[6]*Id.* at 17.
[7]*Id.* at 28.
[8]*Id.*

34. Shortly after he applied for benefits on May 13, 2020, Bozin emailed ODJFS through the website to request his application be cancelled, as he discovered he was eligible to receive unemployment benefits, along with PUA, in another state.

35. On May 15, 2020, Bozin emailed ODJFS through the website to follow-up on his request.

36. On May 20, 2020, Bozin received the Notice from Deloitte.

37. Shortly after receiving the Notice, Bozin was concerned that his identity may have been stolen. Therefore, he purchased credit and identity monitoring software with Lifelock.

38. As a direct result of the Data Breach, Bozin will now have to expend additional time and energy reviewing alerts from Lifelock, verifying his identity with potential creditors, and monitoring his credit, in addition to the monthly service fee he is now paying.

39. Bozin also intends to close financial accounts in the event that these accounts are actually compromised as a result of the Data Breach.

FACTS RELEVANT TO PLAINTIFF TIMOTHY SMITH

40. Smith is a citizen of Ohio (and was during the period of the Data Breach).

41. On May 12, 2020, Smith applied online with the ODJFS for PUA.

42. At the time Smith applied online for PUA, the website was being operated by Deloitte.

43. On May 20, 2020, Smith received the Notice from Deloitte.

44. Shortly after receiving the Notice, Smith was concerned that his identity may have been stolen. Therefore, he purchased credit and identity monitoring software with Lifelock.

45. As a direct result of the Data Breach, Smith will now have to expend additional time and energy reviewing alerts from Lifelock, verifying his identity with potential creditors, and monitoring his credit, in addition to the monthly service fee he is now paying.

46. Smith also intends to close financial accounts in the event that these accounts are actually compromised as a result of the Data Breach.

FACTS RELEVANT TO PLAINTIFF ALEXANDRIA POLICHENA

47. Polichena is a citizen of Ohio (and was during the period of the Data Breach).

48. Prior to May 15, 2020, Polichena applied online with the ODJFS for PUA.

49. At the time Polichena applied online for PUA, the website was being operated by Deloitte.

50. On May 20, 2020, Polichena received the Notice from Deloitte.

51. Shortly after receiving the Notice, Polichena was concerned that her identity may have been stolen. Therefore, she purchased credit and identity monitoring software with Lifelock.

52. As a direct result of the Data Breach, Polichena will now have to expend additional time and energy reviewing alerts from Lifelock, verifying her identity with potential creditors, and monitoring her credit, in addition to the monthly service fee she is now paying.

53. Polichena also intends to close financial accounts in the event that these accounts are actually compromised as a result of the Data Breach.

PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

54. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

55. Plaintiffs and members of the Class have or will suffer actual injury as a direct result of the Data Breach. In addition to fraudulent charges, loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts, and damage to their credit, many victims suffer ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards linked to their bank accounts;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Taking trips to banks and waiting in line to verify their identities in order to restore access to the accounts;

g. Placing "freezes" and "alerts" with credit reporting agencies which, pursuant to ORC 1349.52(I), will cost up to $5.00 per security freeze placed and up to $5.00 per security freeze to be removed;

h. Spending time on the phone with or at the financial institution to dispute fraudulent charges;

i. Contacting their financial institutions and closing or modifying financial accounts;

j. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

k. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

56. Moreover, Plaintiffs and the Class members have an interest in ensuring that their

personal and financial information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

57. In the Notice, Deloitte offers limited guidance to Plaintiffs and Class members other than boilerplate steps that any Ohioan can take in the event of a data breach.

58. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class members have suffered anxiety, emotional distress, loss of privacy, financial damages, and are at an increased risk of future harm.

CLASS ALLEGATIONS

59. **Class Definition**: Plaintiffs bring this action pursuant to Fed. R. Civ. P. 23, on behalf of a statewide class of similarly situated individuals and entities ("the Class"), defined as follows:

> All individuals who applied for pandemic unemployment assistance with the Ohio Department of Job and Family Services, and whose personal information and/or financial information was exposed in the Data Breach.
>
> Excluded from the Class are: (1) Defendant, Defendant's agents, subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest, and those entities' current and former employees, officers, and directors; (2) the Judge to whom this case is assigned and the Judge's immediate family; (3) any person who executes and files a timely request for exclusion from the Class; (4) any persons who have had their claims in this matter finally adjudicated and/or otherwise released; and (5) the legal representatives, successors and assigns of any such excluded person.

60. **Numerosity**: Upon information and belief, the Class is comprised of tens of thousands of members, as it was reported that as many as 161,000 Ohioans had applied for PUA

assistance at the time of the Data Breach.[9] Thus, the Class is so numerous that joinder of all members is impracticable. Class members can easily be identified through Defendant's records, or by other means.

61. **Commonality and Predominance**: There are several questions of law and fact common to the claims of Plaintiffs and Class members, which predominate over any individual issues, including:

a. Whether Defendant adequately protected the personal and financial information of Plaintiffs and members of the Class;

b. Whether Defendant placed the personal and financial information of Plaintiffs and members of the Class in an online storage server without a secure lock on any of the files and was not password-protected;

c. Whether Defendant adopted, implemented, and maintained reasonable policies and procedures to prevent the unauthorized access to the personal and financial information of Plaintiffs and members of the Class;

d. Whether Defendant properly trained and supervised its employees to protect the personal and financial information of Plaintiffs and members of the Class;

e. Whether Defendant promptly notified Plaintiffs and members of the Class of the Data Breach;

f. Whether Defendant owed a duty to Plaintiffs sand members of the Class to safeguard and protect their personal and financial information;

g. Whether Defendant breached a duty to Plaintiffs and members of the Class to safeguard and protect their personal and financial information;

h. Whether Defendant breached a duty to Plaintiffs and members of the Class by failing to adopt, implement, and maintain reasonable policies and procedures to safeguard and protect the personal and financial information of Plaintiffs and members of the Class; and

i. Whether Defendant is liable for the damages suffered by Plaintiffs and members of the Class as a result of the Data Breach.

---

[9] *See, e.g.* Orie Givens, "ODJFS Reports Potential Exposure of PUA Applicant Data" Spectrumnews1.com (May 20, 2020) (last visited May 20, 2020) https://spectrumnews1.com/oh/columbus/news/2020/05/20/odjfs-unemployment-security-issue

62. **Typicality**: Plaintiffs' claims are typical of the claims of members of the Class. All claims are based on the same legal and factual issues. Plaintiffs and each of the Class members provided documents containing their personal and financial information to the ODJFS and Deloitte, and the information was placed in an online storage server that did not have a secure lock and was not password-protected. Defendant's conduct was uniform to Plaintiffs and all Class members.

63. **Adequacy of Representation**: Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class, and have retained counsel competent and experienced in complex class actions. Plaintiffs have no interest antagonistic to those of members of the Class, and Defendant has no defenses unique to Plaintiffs. The questions of law and fact common to the proposed Class predominate over any questions affecting only individual members of the Class.

64. **Superiority**: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for proposed members of the Class to prosecute their claims individually. The trial and the litigation of Plaintiffs' claims are manageable.

COUNT I
Negligence
(On behalf of Plaintiffs and the Class)

65. Plaintiffs repeat and reallege the allegations of paragraphs 1-64 with the same force and effect as though fully set forth herein.

66. Deloitte knew, or should have known, of the risks inherent in collecting and storing the personal and financial information of Plaintiffs and Class members and the

importance of adequate security. Deloitte was well aware of numerous, well-publicized data breaches that exposed the personal and financial information of individuals.

67. Deloitte had a common law duty to prevent foreseeable harm to those whose personal and financial information it was entrusted. This duty existed because Plaintiffs and Class members were the foreseeable and probable victims of the failure of Deloitte to adopt, implement, and maintain reasonable security measures so that Plaintiffs' and Class members' personal and financial information would not be accessible in an unsecured online storage server and not password-protected.

68. Deloitte had a special relationship with Plaintiffs and Class members. Deloitte was entrusted with Plaintiffs' and Class members' documents and electronic data containing their personal and financial information, and Deloitte was in a position to protect the documents and electronic data (and the personal and financial information stored on them) from public exposure.

69. The duties of Deloitte also arose under section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect individuals' personal and financial information by companies. Various FTC publications and data security breach orders further form the basis of the duties of Deloitte.

70. Deloitte had a duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiffs' and Class members' personal and financial information in its possession so that the personal and financial information would not come within the possession, access, or control of unauthorized persons.

71. More specifically, the duties of Deloitte included, among other things, the duty to:

a. Adopt, implement, and maintain policies, procedures, and security measures for protecting documents containing an individual's personal and financial information, including policies, procedures, and security measures to ensure that the documents are not accessible online in unsecured storage servers and are password-protected;

b. Adopt, implement, and maintain reasonable policies and procedures to prevent the sharing of documents containing an individual's personal and financial information with entities that failed to adopt, implement, and maintain policies, procedures, and security measures to ensure that the documents are not accessible online in unsecured storage servers and are password-protected;

c. Adopt, implement, and maintain reasonable policies and procedures to ensure that it is sharing documents containing an individual's personal and financial information only with entities that have adopted, implemented, and maintained policies, procedures, and security measures to ensure that the documents are not accessible online in unsecured storage servers and are password-protected;

d. Properly train its employees to protect documents containing an individual's personal and financial information; and

e. Adopt, implement, and maintain processes to quickly detect a data breach and to promptly act on warnings about data breaches.

72. Deloitte breached the foregoing duties to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the documents and electronic data containing an individual's personal and financial information in its possession so that the documents and electronic data would not come within the possession, access, or control of unauthorized persons. The Notice acknowledges that the personal information of the Plaintiffs and the Class members was exposed in the Data Breach.

73. Deloitte acted with reckless disregard for the security of the personal and financial information of Plaintiffs and the Class because Deloitte knew or should have known

that its data security practices were not adequate to safeguard the personal and financial information that it collected and stored.

74. Deloitte acted with reckless disregard for the rights of Plaintiffs and the Class by failing to promptly detect the Data Breach so that Plaintiffs and the Class members could take measures to protect themselves from damages caused by the unauthorized access of the personal and financial information compromised in the Data Breach.

75. As a result of the conduct of Deloitte, Plaintiffs and Class members have suffered and will continue to suffer actual damages including, but not limited to, expenses and/or time spent on credit monitoring; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts; and increased risk of future harm. Further, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs DANIEL BOZIN, TIMOTHY SMITH, and ALEXANDRIA POLICHENA individually, and on behalf of all others similarly situated, respectfully request that judgment be entered in their favor and against DELOITTE CONSULTING LLP, as follows:

A. That the Court find that this action satisfies the prerequisites for maintenance as a class action and certifying the Class defined herein;

B. That the Court appoint Plaintiffs as representatives of the Class;

C. That the Court appoint Plaintiffs' counsel as counsel for the Class;

D. That the Court enter judgment in favor of Plaintiffs and the Class against Deloitte;

E. That the Court award Plaintiffs and Class members actual damages and all other forms of available relief, as applicable;

F. That the Court award Plaintiffs and Class members punitive damages and all other forms of available relief, as applicable;

G. That the Court award Plaintiffs and the Class attorney's fees and costs, including interest thereon as allowed or required by law;

H. That the Court enter an injunction requiring Deloitte to adopt, implement, and maintain adequate security measures to protect its customers' personal and financial information; and

I. Granting all such further and other relief as the Court deems just and appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs Daniel Bozin, Timothy Smith, and Alexandria Polichena individually, and on behalf of all others similarly situated, hereby demand a trial by jury of all claims so triable.

Respectfully submitted,

/s/ Marc E. Dann
Marc E. Dann (0039425)
Brian D. Flick (0081605)
DANNLAW
P.O. Box 6031040
Cleveland, Ohio 44103
(216) 373-0539 telephone
(216) 373-0536 facsimile
notices@dannlaw.com

Thomas A. Zimmerman, Jr. (*pro hac vice* anticipated)
tom@attorneyzim.com
Matthew C. De Re (*pro hac vice* anticipated)
matt@attorneyzim.com
Jeffrey D. Blake (*pro hac vice* anticipated)
jeff@attorneyzim.com
ZIMMERMAN LAW OFFICES, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
(312) 440-0020 telephone
(312) 440-4180 facsimile
www.attorneyzim.com

Counsel for Plaintiffs and the putative Class

EXHIBIT 1

Dann Law

Brian Flick <bflick@dannlaw.com>

Fwd: Pandemic Unemployment Assistance

1 message

Dan Bozin [redacted]@gmail.com> Wed, May 20, 2020 at 5:56 PM
To: bflick@dannlaw.com

Begin forwarded message:

From: noreply@jfs.ohio.gov
Subject: Pandemic Unemployment Assistance
Date: May 20, 2020 at 2:46:12 PM EDT
To: [redacted]@gmail.com <[redacted]@gmail.com>

May 20, 2020

Dear PUA Applicant:

Deloitte Consulting is currently under contract with the Ohio Department of Job and Family Services (ODJFS) to assist the state of Ohio in administering the Pandemic Unemployment Assistance (PUA) program. Deloitte discovered on May 15, 2020 that your name, Social Security number, and street address pertaining to your application for and receipt of unemployment compensation benefits inadvertently had the capability to be viewed by other unemployment claimants. Thereafter, Deloitte immediately began an investigation and upon discovering the exposure, Deloitte immediately took steps to stop further access to and exposure of your personal information.

At this time, there is no evidence or indication to believe that your personal information was improperly used; therefore, our actions, as well as the actions you may want to consider, are preventative.

As a precaution, you may want to monitor your credit by obtaining a copy of your credit report from one of the three national credit bureaus. Federal law entitles every individual to one free credit report per year from **each** of the three main bureaus.

You may also have a fraud alert placed on your consumer credit file by contacting one of the national credit bureaus. Once one credit bureau places a fraud alert on your credit file, it notifies the other two bureaus. Fraud alerts are typically in effect for 90 days but can be renewed. The credit bureaus may be contacted at:

Equifax: (800) 525-6285 (http://www.equifax.com)
Experian: (888) 397-3742 (http://www.experian.com)
TransUnion: (800) 680-7289 (http://www.tuc.com)

Additionally, Ohio law allows you to place a security freeze on your credit report by contacting one of the bureaus listed above. Should you wish to open a new line of credit while your report is frozen, you may temporarily lift this security freeze by telephone or online by providing a security code. Credit reporting agencies may charge a fee of no more than $5 for each freeze and unfreeze of your report.

If you wish to receive free Experian IdentityWorks identity protection services for the next 12 months, you will receive a follow-up email with enrollment details that will be sent to you via Deloitte or directly from Experian within 3-5 days.

Finally, to find out more about protecting your personal information, visit the Ohio Attorney General's Identity Theft protection page (http://www.ohioattorneygeneral.gov/IdentityTheft) and/or the Federal Trade Commission's identity theft assistance page (https://www.consumer.ftc.gov/features/feature-0014-identity-theft).

We apologize for any concerns or inconvenience as a result of this unauthorized incident. Please be assured that we take very seriously our responsibility to safeguard the personal information you entrust to

our care, and deeply regret that this incident occurred.

If you have questions or concerns that remain unaddressed after reviewing this information, please email: DeloitteIdentityhelp@jfs.ohio.gov.

NAILAH K. BYRD
CUYAHOGA COUNTY CLERK OF COURTS
1200 Ontario Street
Cleveland, Ohio 44113

Court of Common Pleas

New Case Electronically Filed: SERVICE REQUEST
May 21, 2020 13:04

By: MARC E. DANN 0039425

Confirmation Nbr. 2001679

DANIEL BOZIN, ET AL.

vs.

DELOITTE CONSULTING LLP

CV 20 932778

Judge: DAVID T. MATIA

Pages Filed: 1

Common Pleas Court of Cuyahoga County, Ohio
Nailah K. Byrd, Clerk of Courts

INSTRUCTIONS FOR SERVICE

Daniel Bozin, et al.
Plaintiff(s)

Case Number _____

Judge: _____

Vs.
Deloitte Consulting LLP
Defendants(s)

Date: 05/21/2020

Method of Service Requested:

Certified Mail Service ☑ Ordinary Mail Service ☐ Federal Express Service ☑

Personal Service by the Sheriff of _____ County ___

Residence Service by the Sheriff of _____ County ___

Personal Service By Process Server ____

Residence Service by Process Server ____

Name(s) and Address(es) of Parties to Serve:

Deloitte Consulting LLP
c/o Corporation Servicing Company
50 W. Broad Street, Suite 1330
Columbus, OH 43215

Additional Instructions:
Please serve Summons, Complaint and all exhibits

Filing Party Name: Marc E. Dann, Esq. Supreme Court ID if applicable: 0039425

Phone Number: 216-373-0539

For Use by Sheriff or Process Server Only

Number of Service Attempts: _____

Address for Service if Different from address included above

NAILAH K. BYRD
CUYAHOGA COUNTY CLERK OF COURTS
1200 Ontario Street
Cleveland, Ohio 44113

Court of Common Pleas

AMENDED COMPLAINT $75
May 28, 2020 09:05

By: MARC E. DANN 0039425

Confirmation Nbr. 2004283

DANIEL BOZIN, ET AL.

vs.

DELOITTE CONSULTING LLP

CV 20 932778

Judge: DAVID T. MATIA

Pages Filed: 29

IN THE COURT OF COMMON PLEAS
CUYAHOGA COUNTY, OHIO

DANIEL BOZIN, individually and on behalf of all others similarly situated, *et al.* Plaintiffs, v. DELOITTE CONSULTING LLP Defendant.	Case No. CV-20-932778 Judge David T. Matia **FIRST AMENDED CLASS ACTION COMPLAINT FOR DAMAGES** **JURY TRIAL DEMANDED**

Plaintiffs DANIEL BOZIN ("Bozin"), TIMOTHY SMITH ("Smith"), ALEXANDRIA POLICHENA ("Polichena"), BERNADETTE NOLEN ("Nolen"), and NICOLE HORNBECK ("Hornbeck") (collectively, "Plaintiffs"), by and through their attorneys, bring this class action lawsuit on behalf of themselves and all other persons similarly situated, and for their FIRST AMENDED Class Action Complaint against Defendant DELOITTE CONSULTING LLP ("Deloitte" or "Defendant"), Plaintiffs allege with personal knowledge with respect to themselves individually and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters, as follows:

PARTIES

1. Plaintiff DANIEL BOZIN is a natural person with a principal place of residence located in Cuyahoga County, Ohio.

2. Plaintiff TIMOTHY SMITH is a natural person with a principal place of residence in Franklin County, Ohio.

3. Plaintiff ALEXANDRIA POLICHENA is a natural person with a principal place of residence in Portage County, Ohio.

4. Plaintiff BERNADETTE NOLEN is a natural person with a principal place of residence in Trumbull County, Ohio.

5. Plaintiff NICOLE HORNBECK is a natural person with a principal place of residence in Franklin County, Ohio.

6. Defendant DELOITTE CONSULTING LLP is a Delaware limited liability company with a principal place of business in Hermitage, TN.

7. Venue lies in this Court pursuant to Civ. R. 3(B) as a substantial portion of the events that form the basis of this Class Action Complaint occurred in Cuyahoga County, Ohio; Defendant conducted activity that gave rise to the claims for relief in this County; and Defendant maintains an office in this County.

THE DATA BREACH

8. Plaintiffs bring this suit on behalf of themselves and a Class of similarly situated individuals against Defendant for Defendant's failure to secure and protect Plaintiffs' and Class members' personal and financial information.

9. At one of the worst times in the lives of Plaintiffs and Class members, when they find themselves unemployed in the midst of a pandemic and resulting recession, Deloitte was brought in as an expert consultant by certain states, including Colorado, Illinois, and Ohio, to facilitate the secure and efficient processing of Plaintiffs' and Class members' claims for Pandemic Unemployment Assistance ("PUA"). However, Deloitte negligently and recklessly made the Plaintiffs' and Class members' path to recovery significantly harder by putting their

identity and credit standing at risk.

10. On May 20, 2020, Bozin received an email, which is attached as Exhibit 1 to this Complaint (the "Notice").

11. The Notice stated:

> Dear PUA Applicant:
>
> Deloitte Consulting is currently under contract with the Ohio Department of Job and Family Services (ODJFS) to assist the state of Ohio in administering the Pandemic Unemployment Assistance (PUA) program. Deloitte discovered on May 15, 2020 that your name, Social Security number, and street address pertaining to your application for and receipt of unemployment compensation benefits inadvertently had the capability to be viewed by other unemployment claimants. Thereafter, Deloitte immediately began an investigation and upon discovering the exposure, Deloitte immediately took steps to stop further access to and exposure of your personal information.
>
> At this time, there is no evidence or indication to believe that your personal information was improperly used; therefore, our actions, as well as the actions you may want to consider, are preventative.
>
> As a precaution, you may want to monitor your credit by obtaining a copy of your credit report from one of the three national credit bureaus. Federal law entitles every individual to one free credit report per year from each of the three main bureaus.
>
> You may also have a fraud alert placed on your consumer credit file by contacting one of the national credit bureaus. Once one credit bureau places a fraud alert on your credit file, it notifies the other two bureaus. Fraud alerts are typically in effect for 90 days but can be renewed. The credit bureaus may be contacted at:
>
> Equifax: (800) 525-6285 (http://www.equifax.com)
> Experian: (888) 397-3742 (http://www.experian.com)
> TransUnion: (800) 680-7289 (http://www.tuc.com)

> Additionally, Ohio law allows you to place a security freeze on your credit report by contacting one of the bureaus listed above. Should you wish to open a new line of credit while your report is frozen, you may temporarily lift this security freeze by telephone or online by providing a security code. Credit reporting agencies may charge a fee of no more than $5 for each freeze and unfreeze of your report.
>
> If you wish to receive free Experian IdentityWorks identity protection services for the next 12 months, you will receive a follow-up email with enrollment details that will be sent to you via Deloitte or directly from Experian within 3-5 days.
>
> Finally, to find out more about protecting your personal information, visit the Ohio Attorney General's Identity Theft protection page (http://www.ohioattorneygeneral.gov/IdentityTheft) and/or the Federal Trade Commission's identity theft assistance page (https://www.consumer.ftc.gov/features/feature-0014-identitytheft).
> We apologize for any concerns or inconvenience as a result of this unauthorized incident. Please be assured that we take very seriously our responsibility to safeguard the personal information you entrust to our care, and deeply regret that this incident occurred.
>
> If you have questions or concerns that remain unaddressed after reviewing this information, please email:
> DeloitteIdentityhelp@jfs.ohio.gov.

See Exhibit 1 at pp. 1-2.

12. On May 20, 2020, the same Notice was sent to Smith via e-mail.

13. On May 20, 2020, the same Notice was sent to Polichena via e-mail.

14. On May 20, 2020, the same Notice was sent to Nolen via e-mail.

15. On May 20,2020, the same Notice was sent to Hornbeck via e-mail.

16. The Notice acknowledges that a treasure trove of highly sensitive personal information was subject to unauthorized access by numerous third parties (the "Data Breach").

See Exhibit 1 at p. 1.

17. As a result of the Data Breach, Plaintiffs and Class members must now be vigilant and review their credit reports for incidents of identity theft, and to educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft.

18. Data security breaches have dominated the headlines for the last two decades, and it does not take an IT industry expert to know that major businesses who fail to take reasonable security precautions like Deloitte are at risk.

19. The general public can tell you the names of some of the biggest data breaches: LabCorp, Quest Diagnostics, Yahoo, Equifax, Marriott International, Target, Home Depot, Anthem, Heartland Payment Systems, and TJX Companies, Inc.[1]

20. Deloitte is no stranger to data breaches and phishing scams of its own employees.[2]

21. Upon information and belief, Deloitte failed to implement reasonable industry standards necessary to prevent a data breach, including the FTC's guidelines, resulting in the Data Breach.

22. Likewise, Deloitte failed to create, maintain, and/or comply with a written cybersecurity program that incorporated physical, technical, and administrative safeguards for the protection of personal information and reasonably conformed to an industry recognized cybersecurity framework, resulting in the Data Breach.

---

[1] S*ee, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[2] *See, e.g., Source: Deloitte Breach Affected All Company Email, Admin Accounts*, Krebsonsecurity.com (September 25, 2017) (last visited May 20, 2020) https://krebsonsecurity.com/2017/09/source-deloitte-breach-affected-all-company-email-admin-accounts/

23. Because of its failure to create, maintain, and/or comply with a necessary cybersecurity program, Deloitte was unable to ensure the protection of information security and confidentiality, and protect against obvious and readily foreseeable threats to information security and confidentiality or the unauthorized access to the personal and financial information, resulting in the Data Breach.

DAMAGES FROM DATA BREACHES

24. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[3]

25. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[4]

26. Identity thieves use stolen personal information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

27. Identity thieves can also use SSNs to obtain a driver's license or official

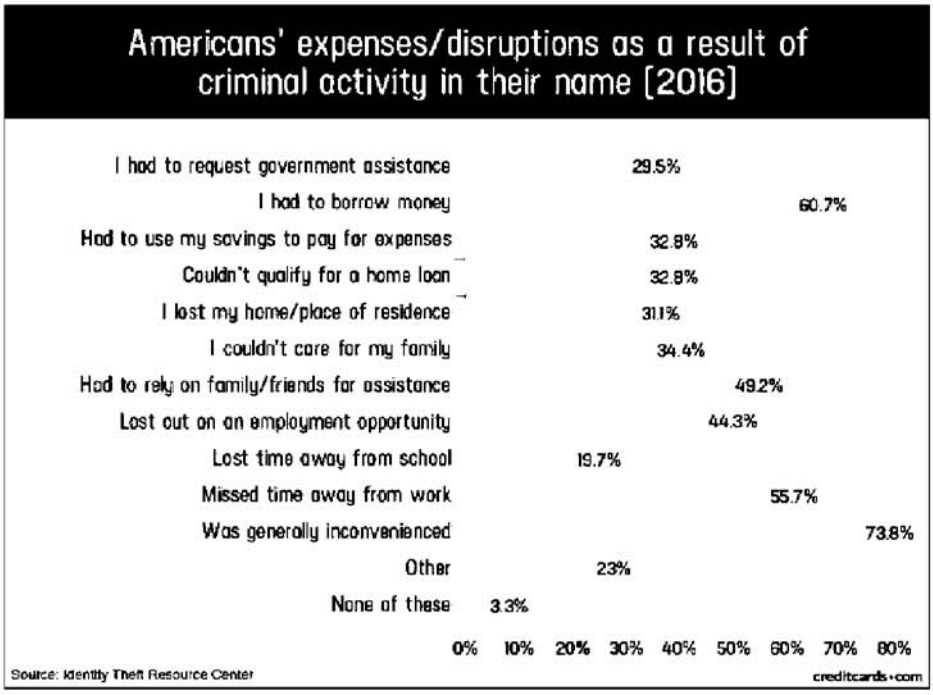
---

[3] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," pg. 2, by U.S. Government Accountability Office, June 2007, at: https://www.gao.gov/new.items/d07737.pdf (last visited May 20, 2020) ("GAO Report").

[4] *See* https://www.identitytheft.gov/Steps (last visited May 20, 2020).

identification card in the victim's name but with the thief's picture; use the victim's name and SSN to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

28. A study by the Identity Theft Resource Center show the multitude of harms caused by fraudulent use of personal and financial information:



Source: "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/17, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited May 20, 2020).

29. There may be a time lag between when harm occurs versus when it is discovered, and also between when personal and financial information is stolen and when it is used.

According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

30. Personal and financial information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

31. Thus, there is a strong probability that entire batches of stolen information have been dumped on the black market, and are yet to be dumped on the black market, meaning Plaintiffs and Class members are at an increased risk of fraud and identity theft for many years into the future.

32. Data breaches are preventable.[5] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[6] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[7]

---

[5]Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[6]*Id.* at 17.
[7]*Id.* at 28.

33. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[8]

FACTS RELEVANT TO PLAINTIFF DANIEL BOZIN

34. Bozin is a citizen of Ohio (and was during the period of the Data Breach).

35. On May 13, 2020, Bozin applied online with the Ohio Department of Job and Family Services ("ODJFS") for pandemic unemployment assistance ("PUA").

36. At the time Bozin applied online for PUA, the website was being operated by Deloitte.

37. Shortly after he applied for benefits on May 13, 2020, Bozin emailed ODJFS through the website to request his application be cancelled, as he discovered he was eligible to receive unemployment benefits, along with PUA, in another state.

38. On May 15, 2020, Bozin emailed ODJFS through the website to follow up on his request.

39. On May 20, 2020, Bozin received the Notice.

40. Shortly after receiving the Notice, Bozin was concerned that his identity may have been stolen. Therefore, he purchased credit and identity monitoring software with Lifelock.

41. As a direct result of the Data Breach, Bozin will now have to expend additional time and energy reviewing alerts from Lifelock, verifying his identity with potential creditors, and monitoring his credit, in addition to the monthly service fee he is now paying.

---

[8] *Id.*

42. Bozin also intends to close financial accounts in the event that these accounts are actually compromised as a result of the Data Breach.

FACTS RELEVANT TO PLAINTIFF TIMOTHY SMITH

43. Smith is a citizen of Ohio (and was during the period of the Data Breach).

44. On May 12, 2020, Smith applied online with the ODJFS for PUA.

45. At the time Smith applied online for PUA, the website was being operated by Deloitte.

46. On May 20, 2020, Smith received the Notice.

47. Shortly after receiving the Notice, Smith was concerned that his identity may have been stolen. Therefore, he purchased credit and identity monitoring software with Lifelock.

48. As a direct result of the Data Breach, Smith will now have to expend additional time and energy reviewing alerts from Lifelock, verifying his identity with potential creditors, and monitoring his credit, in addition to the monthly service fee he is now paying.

49. Smith also intends to close financial accounts in the event that these accounts are actually compromised as a result of the Data Breach.

FACTS RELEVANT TO PLAINTIFF ALEXANDRIA POLICHENA

50. Polichena is a citizen of Ohio (and was during the period of the Data Breach).

51. Prior to May 15, 2020, Polichena applied online with the ODJFS for PUA.

52. At the time Polichena applied online for PUA, the website was being operated by Deloitte.

53. On May 20, 2020, Polichena received the Notice.

54. Shortly after receiving the Notice, Polichena was concerned that her identity may have been stolen. Therefore, she purchased credit and identity monitoring software with Lifelock.

55. As a direct result of the Data Breach, Polichena will now have to expend additional time and energy reviewing alerts from Lifelock, verifying her identity with potential creditors, and monitoring her credit, in addition to the monthly service fee she is now paying.

56. Polichena also intends to close financial accounts in the event that these accounts are actually compromised as a result of the Data Breach.

FACTS RELEVANT TO PLAINTIFF BERNADETTE NOLEN

57. Nolen is a citizen of Ohio (and was during the period of the Data Breach).

58. At the time Nolen applied online with the ODJFS, the website was being operated by Deloitte.

59. On or around May 20, 2020, Nolen received the Notice.

60. On May 22, 2020, Nolen received PUA funds and they were directly deposited into her Netspend account, where she had requested the money be deposited.

61. On May 23, 2020, Nolen received a text alert from Netspend stating that her card was reported stolen.

62. Nolen had her card with her at the time she received the text alert from Netspend, and she had not reported it stolen.

63. Nolen immediately called Netspend and the representative stated that her account was locked and her card had been canceled. Nolen was told that a new card would be sent to her in one week, and she would be without access to much needed funds in the meantime.

64. A few hours later, Nolen received an e-mail from Netspend notifying her of a transfer of a substantial amount of money from her supposedly locked account to another account. Nolen had only one authorized account at the time—the account the money was transferred from—and she did not authorize the transfer reported in the e-mail and did not own the account the money was being transferred to.

65. Nolen immediately called Netspend to dispute the transfer, and she spent approximately an hour and a half on the phone with a Netspend representative attempting to understand what occurred, explain her predicament, and rectify the situation. During this phone call, she was told Netspend had three accounts in her name. The dispute is currently pending an internal investigation that could take months to resolve, according to Netspend.

66. In addition, Nolen was notified that a substantial sum of money was wired by Western Union from her Netspend account. She immediately called a Western Union representative but was unable to get very far. The representative required a reference number to proceed that Nolen did not have. Nolen disputed the charge, and the dispute is currently pending Western Union's investigation.

67. On May 24, 2020, Nolen again spoke with a Netspend representative and she was informed that an unauthorized person was attempting to order new cards associated with her Netspend account.

68. In addition, Nolen was notified that her phone account was switched from her Boostmobile account to Metro using her personal and financial information. Nolen did not authorize the switch. She now has a new phone, and the phone is not in her name for her protection.

69. Nolen spent time and effort to file a police report relating to these events for her protection and to secure her information going forward. While the significant issues with Nolen's funds are being disputed, Nolen is deprived of urgently needed money to provide for her childrens' basic needs, including healthcare, as well as her own.

FACTS RELEVANT TO PLAINTIFF NICOLE HORNBECK

70. Hornbeck is a citizen of Ohio (and was during the period of the Data Breach).

71. On May 12, 2020, Hornbeck filed an application for PUA. She elected to receive her benefits by direct deposit to her Netspend bank account.

72. On May 20, 2020, Hornbeck received an email notifying her that her personal and financial information was exposed in the Data Breach.

73. On May 21, 2020, Hornbeck received her PUA benefits, which were directly deposited in her Netspend account.

74. Later that day, Hornbeck received an alert from Netspend that her bank card was reported stolen. Hornbeck knew it was not physically stolen, because she had it in her possession.

75. Hornbeck immediately attempted to login to her bank account, but her login credentials would not provide her access to her account.

76. Hornbeck called her bank concerned about the security of her account. She provided her credentials and correctly answered the security questions, reset her credentials, and ordered a new bank card to be delivered to replace her now canceled card. She was without the use of her card until her canceled card would be replaced.

77. The next day, on May 22, 2020, Hornbeck discovered that, using her updated account information, she was again locked out of her account.

78. In a follow up conversation with a Netspend representative, Netspend informed Hornbeck that, after ten years of banking with Netspend, Netspend decided to end their banking relationship. Netspend informed Hornbeck that it would send by mail a check for the money in her account that would reach her in 7–10 business days. Until Hornbeck receives her check, she will not have access to the money in her account, which is her primary account for making purchases, and which includes her much-needed PUA benefits.

79. In addition, Hornbeck received two alerts from her phone company, Boostmobile, that the pin on her account was requested. She had not requested her pin, nor authorized another person to do so. She made a phone call to Boostmobile to inquire and ensure her account was secure.

PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

80. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

81. Plaintiffs and members of the Class have or will suffer actual injury as a direct result of the Data Breach. In addition to fraudulent charges, loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts, and damage to their credit, many victims suffer ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards linked to their bank accounts;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Taking trips to banks and waiting in line to verify their identities in order to restore access to the accounts;

g. Placing "freezes" and "alerts" with credit reporting agencies which, pursuant to ORC 1349.52(I), will cost up to $5.00 per security freeze placed and up to $5.00 per security freeze to be removed;

h. Spending time on the phone with or at the financial institution to dispute fraudulent charges;

i. Contacting their financial institutions and closing or modifying financial accounts;

j. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

k. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

82. Moreover, Plaintiffs and the Class members have an interest in ensuring that their personal and financial information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

83. In the Notice, Plaintiffs and Class members are given minimal information, other

than boilerplate steps that any person can take in the event of a data breach.

84. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class members have suffered anxiety, emotional distress, loss of privacy, financial damages, and are at an increased risk of future harm.

CLASS ALLEGATIONS

85. **Class Definition**: Plaintiffs bring this action pursuant to Fed. R. Civ. P. 23, on behalf of a class of similarly situated individuals and entities ("the Class"), defined as follows:

> All individuals who applied for Pandemic Unemployment Assistance, including with the Colorado Department of Labor and Employment, Illinois Department of Employment Security, and Ohio Department of Job and Family Services, and whose personal information and/or financial information was exposed in the Data Breach.
>
> Excluded from the Class are: (1) Defendant, Defendant's agents, subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest, and those entities' current and former employees, officers, and directors; (2) the Judge to whom this case is assigned and the Judge's immediate family; (3) any person who executes and files a timely request for exclusion from the Class; (4) any persons who have had their claims in this matter finally adjudicated and/or otherwise released; and (5) the legal representatives, successors and assigns of any such excluded person.

86. **Numerosity**: Upon information and belief, the Class is comprised of hundreds of thousands of members. The actual number is unknown at present. Initial reports state that approximately 72,000 Coloradans, 32,500 Illinoisans, and 130,000 Ohioans had sensitive and confidential information exposed.[9] Thus, the Class is so numerous that joinder of all members is

---

[9] *See* https://www.kktv.com/content/news/Colorado-Labor-Department-confirms-brief-data-exposure-for-pandemic-unemployment-claimants-570633261.html; https://www.illinoispolicy.org/state-agency-published-private-data-of-nearly-32500-unemployed-illinoisans/;

impracticable. Class members can easily be identified through Defendant's records, or by other means.

87. **Commonality and Predominance**: There are several questions of law and fact common to the claims of Plaintiffs and Class members, which predominate over any individual issues, including:

a. Whether Defendant adequately protected the personal and financial information of Plaintiffs and members of the Class;

b. Whether Defendant placed the personal and financial information of Plaintiffs and members of the Class in an online storage server without a secure lock on any of the files and was not password-protected;

c. Whether Defendant adopted, implemented, and maintained reasonable policies and procedures to prevent the unauthorized access to the personal and financial information of Plaintiffs and members of the Class;

d. Whether Defendant properly trained and supervised its employees to protect the personal and financial information of Plaintiffs and members of the Class;

e. Whether Defendant promptly notified Plaintiffs and members of the Class of the Data Breach;

f. Whether Defendant owed a duty to Plaintiffs sand members of the Class to safeguard and protect their personal and financial information;

g. Whether Defendant breached a duty to Plaintiffs and members of the Class to safeguard and protect their personal and financial information;

h. Whether Defendant breached a duty to Plaintiffs and members of the Class by failing to adopt, implement, and maintain reasonable policies and procedures to safeguard and protect the personal and financial information of Plaintiffs and members of the Class; and

i. Whether Defendant is liable for the damages suffered by Plaintiffs and members of the Class as a result of the Data Breach.

---

https://www.wlwt.com/article/unemployment-data-system-breach-in-ohio-puts-thousands-of-applicants-info-at-potential-risk/32620720 (last visited May, 22, 2020).

88. **Typicality**: Plaintiffs' claims are typical of the claims of members of the Class. All claims are based on the same legal and factual issues. Plaintiffs and each of the Class members provided their personal and financial information to Deloitte, and the information was placed in an online storage server that did not have a secure lock and was not password-protected. Defendant's conduct was uniform to Plaintiffs and all Class members.

89. **Adequacy of Representation**: Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class, and have retained counsel competent and experienced in complex class actions. Plaintiffs have no interest antagonistic to those of members of the Class, and Defendant has no defenses unique to Plaintiffs. The questions of law and fact common to the proposed Class predominate over any questions affecting only individual members of the Class.

90. **Superiority**: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for proposed members of the Class to prosecute their claims individually. The trial and the litigation of Plaintiffs' claims are manageable.

COUNT I
Negligence
(On behalf of Plaintiffs and the Class)

91. Plaintiffs repeat and reallege the allegations of paragraphs 1-90 with the same force and effect as though fully set forth herein.

92. Deloitte knew, or should have known, of the risks inherent in collecting and storing the personal and financial information of Plaintiffs and Class members and the

importance of adequate security. Deloitte was well aware of numerous, well-publicized data breaches that exposed the personal and financial information of individuals.

93. Deloitte had a common law duty to prevent foreseeable harm to those whose personal and financial information it was entrusted. This duty existed because Plaintiffs and Class members were the foreseeable and probable victims of the failure of Deloitte to adopt, implement, and maintain reasonable security measures so that Plaintiffs' and Class members' personal and financial information would not be accessible in an unsecured online storage server and not password-protected.

94. Deloitte had a special relationship with Plaintiffs and Class members. Deloitte was entrusted with Plaintiffs' and Class members' documents and electronic data containing their personal and financial information, and Deloitte was in a position to protect the documents and electronic data (and the personal and financial information stored on them) from public exposure.

95. The duties of Deloitte also arose under section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect individuals' personal and financial information by companies. Various FTC publications and data security breach orders further form the basis of the duties of Deloitte.

96. Deloitte had a duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiffs' and Class members' personal and financial

information in its possession so that the personal and financial information would not come within the possession, access, or control of unauthorized persons.

97. More specifically, the duties of Deloitte included, among other things, the duty to:

a. Adopt, implement, and maintain policies, procedures, and security measures for protecting documents containing an individual's personal and financial information, including policies, procedures, and security measures to ensure that the documents are not accessible online in unsecured storage servers and are password-protected;

b. Adopt, implement, and maintain reasonable policies and procedures to prevent the sharing of documents containing an individual's personal and financial information with entities that failed to adopt, implement, and maintain policies, procedures, and security measures to ensure that the documents are not accessible online in unsecured storage servers and are password-protected;

c. Adopt, implement, and maintain reasonable policies and procedures to ensure that it is sharing documents containing an individual's personal and financial information only with entities that have adopted, implemented, and maintained policies, procedures, and security measures to ensure that the documents are not accessible online in unsecured storage servers and are password-protected;

d. Properly train its employees to protect documents containing an individual's personal and financial information; and

e. Adopt, implement, and maintain processes to quickly detect a data breach and to promptly act on warnings about data breaches.

98. Deloitte breached the foregoing duties to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the documents and electronic data containing an individual's personal and financial information in its possession so that the documents and electronic data would not come within the possession, access, or control of unauthorized persons. The Notice acknowledges that the personal information of the Plaintiffs and the Class members was exposed in the Data Breach. The experiences of Plaintiffs shows

that their personal and financial information was accessed and misused by unauthorized third parties.

99. Deloitte acted with reckless disregard for the security of the personal and financial information of Plaintiffs and the Class because Deloitte knew or should have known that its data security practices were not adequate to safeguard the personal and financial information that it collected and stored.

100. Deloitte acted with reckless disregard for the rights of Plaintiffs and the Class by failing to promptly detect the Data Breach so that Plaintiffs and the Class members could take measures to protect themselves from damages caused by the unauthorized access of the personal and financial information compromised in the Data Breach.

101. Deloitte's data security violations were so egregious that numerous unauthorized persons were able to—and actually did—easily navigate to Deloitte's website(s), and view, access, download, and disseminate reams of personally identifiable and financially valuable information of tens of thousands of people all at once.

102. At least some of these unauthorized persons were able to—and actually did—transmit and further disseminate the personally identifiable and financially valuable information of tens of thousands of people all at once.

103. As a result of the conduct of Deloitte, Plaintiffs and Class members have suffered and will continue to suffer actual damages including, but not limited to, expenses and/or time spent on credit monitoring; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts; and increased risk of future harm. Further, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury

and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT II
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

104. Plaintiffs repeat and reallege the allegations of paragraphs 1–90 with the same force and effect as though fully set forth herein.

105. Defendant invaded the right to privacy of Plaintiffs and Class members by displaying, disclosing, and allowing unfettered access of their personal and financial information to unauthorized and unknown individuals, and by failing to employ reasonable and necessary safeguards to prevent unauthorized access to Plaintiffs' and Class members' personal and financial information.

106. Plaintiffs' and Class members' personal and financial information was held privately and confidentially by them, and used only for legitimate personal and financial purposes. They only entrusted their personal and financial information with third parties as necessary for legitimate purposes, and required the third parties to hold the personal and financial information in confidence at all times and protect it against unauthorized disclosures. Plaintiffs and Class members were reasonable in expecting Defendant to maintain the security and confidentiality of their personal and financial information.

107. Defendant's conduct was and is highly offensive to a reasonable person with ordinary sensibilities.

108. As a result of the conduct of Deloitte, Plaintiffs and Class members have suffered and will continue to suffer actual damages including, but not limited to, expenses and/or time

spent on credit monitoring; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts; and increased risk of future harm. Further, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT III
Injunctive Relief
(On Behalf of Plaintiffs and the Class)

109. Plaintiffs repeat and reallege the allegations of paragraphs 1–90 with the same force and effect as though fully set forth herein.

110. Defendant's ongoing and continuing wrongful conduct, including its failures to employ reasonably adequate security over Plaintiffs' and Class' members' personal and financial information and failures to adequately remedy the effects of the Data Breach, has caused and will continue to cause Plaintiffs and Class members to suffer irreparable harm, including but not limited to: fraudulent charges, fraudulent activity relating to opening new accounts for credit, loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts, damage to their credit, out-of-pocket expenses, the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

111. Such irreparable harm will not cease unless enjoined by the Court.

112. Plaintiffs and the Class are entitled to injunctive relief and other affirmative equitable relief, including, but not limited to: an order compelling Defendant to: (i) notify each person whose personal and financial information was in Defendant's possession during the Data

Breach; (ii) provide credit monitoring protection for each such person without opting in and at no cost to the person for a reasonable time period exceeding one year; (iii) secure its computer environment containing Plaintiffs' and Class members' personal and financial information, and to implement and continuously employ industry standard and reasonable security procedures for the protection of their personal and financial information; and (iv) require independent third party audits for a reasonable period of time going forward to ensure that Defendant maintains reasonable industry standard data security practices.

113. If the requested injunction is not issued, Plaintiffs and the Class will suffer and continue to suffer irreparable injury in the form of continued exposure of their personal and financial information, further dissemination of their personal and financial information, and identity theft and fraud. In addition, Defendant is subject to another cyber attack now that its insufficient data security practices are known. The threat of a future data breach exposing Plaintiffs' and Class members' personal and financial information is immediate, substantial, and real.

114. The hardship to Plaintiffs and Class members were the injunction not to issue would be significant. Defendant continues to possess and handle Plaintiffs' and Class members' personal and financial information. Plaintiffs and Class members bear the brunt of harm of another data breach, while Defendant does not suffer real loss.

115. The requested injunctive relief is in the public interest, as it will provide assurances and security to Plaintiffs and Class members who are already vulnerable and in need of assistance, and will facilitate the increased participation in the PUA program, which exists for the purpose of aiding Plaintiffs and the Class, as well as future applicants and the economy.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs DANIEL BOZIN, TIMOTHY SMITH, ALEXANDRIA POLICHENA, BERNADETTE NOLEN, and NICOLE HORNBECK, individually, and on behalf of all others similarly situated, respectfully request that judgment be entered in their favor and against DELOITTE CONSULTING LLP, as follows:

A. That the Court find that this action satisfies the prerequisites for maintenance as a class action and certifying the Class defined herein;

B. That the Court appoint Plaintiffs as representatives of the Class;

C. That the Court appoint Plaintiffs' counsel as counsel for the Class;

D. That the Court enter judgment in favor of Plaintiffs and the Class against Deloitte;

E. That the Court award Plaintiffs and Class members actual damages and all other forms of available relief, as applicable;

F. That the Court award Plaintiffs and Class members punitive damages and all other forms of available relief, as applicable;

G. That the Court award Plaintiffs and the Class attorney's fees and costs, including interest thereon as allowed or required by law;

H. That the Court enter an injunction as set forth above, including requiring Deloitte to adopt, implement, and maintain adequate security measures to protect Plaintiffs' and Class members' personal and financial information; and

I. Granting all such further and other relief as the Court deems just and appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs Daniel Bozin, Timothy Smith, Alexandria Polichena, Bernadette Nolen, and Nicole Hornbeck, individually, and on behalf of all others similarly situated, hereby demand a trial by jury of all claims so triable.

Respectfully submitted,

/s/ Marc Dann
Marc E. Dann (0039425)
Brian D. Flick (0081605)
DannLaw
P.O. Box 6031040
Cleveland, Ohio 44103
(216) 373-0539 telephone
(216) 373-0536 facsimile
notices@dannlaw.com

Thomas A. Zimmerman, Jr. (*pro hac vice* anticipated)
tom@attorneyzim.com
Zimmerman Law Offices, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
(312) 440-0020 telephone
(312) 440-4180 facsimile
www.attorneyzim.com

Counsel for Plaintiffs and the putative Class

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing *Plaintiffs' First Amended Class Action Complaint for Damages* was electronically filed with the Cuyahoga County Court of Common Pleas on May 28, 2020 and served upon the following parties via electronic mail at the address listed below:

Daniel Warren, Esq. at dwarren@bakerlaw.com Baker & Hostettler LLP
127 Public Square, Suite 200
Cleveland, OH 44114
Counsel for Defendant Deloitte Consulting LLP

and upon the following party via ordinary first-class mail on May 28, 2020:

Deloitte Consulting LLP
c/o Corporation Servicing Company
50 W. Broad St, Suite 1330
Columbus, OH 43215

/s/ Marc Dann
Marc E. Dann (0039425)
Brian D. Flick (0081605)
DannLaw
Counsel for Plaintiffs and the putative Class

EXHIBIT 1

Dann Law

Brian Flick <bflick@dannlaw.com>

Fwd: Pandemic Unemployment Assistance

1 message

Dan Bozin [redacted]@gmail.com> Wed, May 20, 2020 at 5:56 PM
To: bflick@dannlaw.com

Begin forwarded message:

From: noreply@jfs.ohio.gov
Subject: Pandemic Unemployment Assistance
Date: May 20, 2020 at 2:46:12 PM EDT
To: [redacted]@gmail.com <[redacted]@gmail.com>

May 20, 2020

Dear PUA Applicant:

Deloitte Consulting is currently under contract with the Ohio Department of Job and Family Services (ODJFS) to assist the state of Ohio in administering the Pandemic Unemployment Assistance (PUA) program. Deloitte discovered on May 15, 2020 that your name, Social Security number, and street address pertaining to your application for and receipt of unemployment compensation benefits inadvertently had the capability to be viewed by other unemployment claimants. Thereafter, Deloitte immediately began an investigation and upon discovering the exposure, Deloitte immediately took steps to stop further access to and exposure of your personal information.

At this time, there is no evidence or indication to believe that your personal information was improperly used; therefore, our actions, as well as the actions you may want to consider, are preventative.

As a precaution, you may want to monitor your credit by obtaining a copy of your credit report from one of the three national credit bureaus. Federal law entitles every individual to one free credit report per year from **each** of the three main bureaus.

You may also have a fraud alert placed on your consumer credit file by contacting one of the national credit bureaus. Once one credit bureau places a fraud alert on your credit file, it notifies the other two bureaus. Fraud alerts are typically in effect for 90 days but can be renewed. The credit bureaus may be contacted at:

Equifax: (800) 525-6285 (http://www.equifax.com)
Experian: (888) 397-3742 (http://www.experian.com)
TransUnion: (800) 680-7289 (http://www.tuc.com)

Additionally, Ohio law allows you to place a security freeze on your credit report by contacting one of the bureaus listed above. Should you wish to open a new line of credit while your report is frozen, you may temporarily lift this security freeze by telephone or online by providing a security code. Credit reporting agencies may charge a fee of no more than $5 for each freeze and unfreeze of your report.

If you wish to receive free Experian IdentityWorks identity protection services for the next 12 months, you will receive a follow-up email with enrollment details that will be sent to you via Deloitte or directly from Experian within 3-5 days.

Finally, to find out more about protecting your personal information, visit the Ohio Attorney General's Identity Theft protection page (http://www.ohioattorneygeneral.gov/IdentityTheft) and/or the Federal Trade Commission's identity theft assistance page (https://www.consumer.ftc.gov/features/feature-0014-identity-theft).

We apologize for any concerns or inconvenience as a result of this unauthorized incident. Please be assured that we take very seriously our responsibility to safeguard the personal information you entrust to

our care, and deeply regret that this incident occurred.

If you have questions or concerns that remain unaddressed after reviewing this information, please email: DeloitteIdentityhelp@jfs.ohio.gov.

Motion No. 4867903

NAILAH K. BYRD
CUYAHOGA COUNTY CLERK OF COURTS
1200 Ontario Street
Cleveland, Ohio 44113

Court of Common Pleas

MOTION FOR TEMPORARY RESTRAINING ORDER
May 28, 2020 15:04

By: MARC E. DANN 0039425

Confirmation Nbr. 2004806

DANIEL BOZIN, ET AL.

vs.

DELOITTE CONSULTING LLP

CV 20 932778

Judge: DAVID T. MATIA

Pages Filed: 64

IN THE COURT OF COMMON PLEAS
CUYAHOGA COUNTY, OHIO

DANIEL BOZIN, individually and on behalf of all others similarly situated, *et al.* Plaintiffs, v. DELOITTE CONSULTING LLP Defendant.	Case No.: CV 20 932778 Judge David T. Matia

PLAINTIFFS' EMERGENCY MOTION PURSUANT TO CIV. R. 65 FOR A TEMPORARY RESTRAINING ORDER AND/OR PRELIMINARY INJUNCTION

NOW COME Plaintiffs DANIEL BOZIN ("Bozin"), TIMOTHY SMITH ("Smith"), ALEXANDRIA POLICHENA ("Polichena"), BERNADETTE NOLEN ("Nolen"), and NICOLE HORNBECK ("Hornbeck") (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, by and through counsel, and bring their *Emergency Motion Pursuant to Civ. R. 65 for a Temporary Restraining Order and/or Preliminary Injunction* ("Motion"). Defendant has retained counsel, and Plaintiffs' counsel have provided notice of this Motion. In support of this Motion, Plaintiffs state as follows:

I. FACTUAL BASIS FOR THE MOTION.

A. The Data Breach.

Plaintiffs brought this action, for themselves and on behalf of a Class[1], against Defendant DELOITTE CONSULTING LLP ("Deloitte" or "Defendant") for its actions and inactions that resulted in a data breach affecting applicants to the Pandemic Unemployment Assistance ("PUA") program in Ohio and other states. At one of the worst times in the lives of Plaintiffs and Class members, when they find themselves unemployed in the midst of a pandemic and resulting recession, Deloitte was brought in as an expert consultant by certain states, including Colorado, Illinois, and Ohio, to facilitate the secure and efficient processing of Plaintiffs' and Class members' claims for PUA. Compl. ¶ 8. However, Deloitte negligently and recklessly made Plaintiffs' and Class members' path to recovery significantly harder by putting their identity and credit standing at risk. *Id.* Deloitte has exposed and failed to protect Plaintiffs' and other PUA applicants' personal and financial information, including their names, Social Security numbers, and street addresses, and potentially other personal and financial information, as well as private information that applicants were required to provide on behalf of members of their families.

On May 20, 2020, Plaintiffs each received an email with the same Notice attached thereto. *See* Compl. ¶¶ 10-15. The Notice acknowledges that highly sensitive personal information was subject to unauthorized access by numerous third parties (the "Data Breach"). *See* Exhibit 1 to the Complaint (the "Notice"). The Notice stated:

> Dear PUA Applicant:
>
> Deloitte Consulting is currently under contract with the Ohio Department

[1] Plaintiffs seek certify of a Class defined as follows: "All individuals who applied for Pandemic Unemployment Assistance, including with the Colorado Department of Labor and Employment, Illinois Department of Employment Security, and Ohio Department of Job and Family Services, and whose personal information and/or financial information was exposed in the Data Breach." *See* Amended Class Action Complaint ("Complaint" or "Compl."), attached hereto as **Exhibit A**, ¶ 85.

of Job and Family Services (ODJFS) to assist the state of Ohio in administering the Pandemic Unemployment Assistance (PUA) program. Deloitte discovered on May 15, 2020 that your name, Social Security number, and street address pertaining to your application for and receipt of unemployment compensation benefits inadvertently had the capability to be viewed by other unemployment claimants. Thereafter, Deloitte immediately began an investigation and upon discovering the exposure, Deloitte immediately took steps to stop further access to and exposure of your personal information.

At this time, there is no evidence or indication to believe that your personal information was improperly used; therefore, our actions, as well as the actions you may want to consider, are preventative.

As a precaution, you may want to monitor your credit by obtaining a copy of your credit report from one of the three national credit bureaus. Federal law entitles every individual to one free credit report per year from each of the three main bureaus.

You may also have a fraud alert placed on your consumer credit file by contacting one of the national credit bureaus. Once one credit bureau places a fraud alert on your credit file, it notifies the other two bureaus. Fraud alerts are typically in effect for 90 days but can be renewed. The credit bureaus may be contacted at:

Equifax: (800) 525-6285 (http://www.equifax.com)
Experian: (888) 397-3742 (http://www.experian.com)
TransUnion: (800) 680-7289 (http://www.tuc.com)

Additionally, Ohio law allows you to place a security freeze on your credit report by contacting one of the bureaus listed above. Should you wish to open a new line of credit while your report is frozen, you may temporarily lift this security freeze by telephone or online by providing a security code. Credit reporting agencies may charge a fee of no more than $5 for each freeze and unfreeze of your report.

If you wish to receive free Experian IdentityWorks identity protection services for the next 12 months, you will receive a follow-up email with enrollment details that will be sent to you via Deloitte or directly from

> Experian within 3-5 days.
>
> Finally, to find out more about protecting your personal information, visit the Ohio Attorney General's Identity Theft protection page (http://www.ohioattorneygeneral.gov/IdentityTheft) and/or the Federal Trade Commission's identity theft assistance page (https://www.consumer.ftc.gov/features/feature-0014-identitytheft). We apologize for any concerns or inconvenience as a result of this unauthorized incident. Please be assured that we take very seriously our responsibility to safeguard the personal information you entrust to our care, and deeply regret that this incident occurred.
>
> If you have questions or concerns that remain unaddressed after reviewing this information, please email: DeloitteIdentityhelp@jfs.ohio.gov.

See Compl. at Exhibit 1 at pp. 1-2.

Upon information and belief, Deloitte failed to implement reasonable industry standards necessary to prevent a data breach, including the FTC's guidelines, resulting in the Data Breach. Compl. ¶ 21. Likewise, Deloitte failed to create, maintain, and/or comply with a written cybersecurity program that incorporated physical, technical, and administrative safeguards for the protection of personal and financial information and reasonably conformed to an industry recognized cybersecurity framework, resulting in the Data Breach. *Id.* ¶ 22. Because of its failure to create, maintain, and/or comply with a necessary cybersecurity program, Deloitte was unable to ensure the protection of information security and confidentiality, protect against obvious and readily foreseeable threats to information security and confidentiality or the unauthorized access of the Plaintiffs' and Class members' personal and financial information, resulting in the Data Breach. *Id.* ¶ 23.

It has been reported that the personal and financial information of PUA applicants was

viewable online as recently as May 24, 2020, which is nine days after Deloitte reported that it discovered the Data Breach and "immediately took steps to stop further access to and exposure of your personal information." *See* Affidavit of Brian Flick in Support of Plaintiffs' Emergency Motion Pursuant to Civ. R. 65 for a Temporary Restraining Order and/or Preliminary Injunction, attached hereto as **Exhibit B**.

B. Damages from Data Breaches.

The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[2] The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[3]

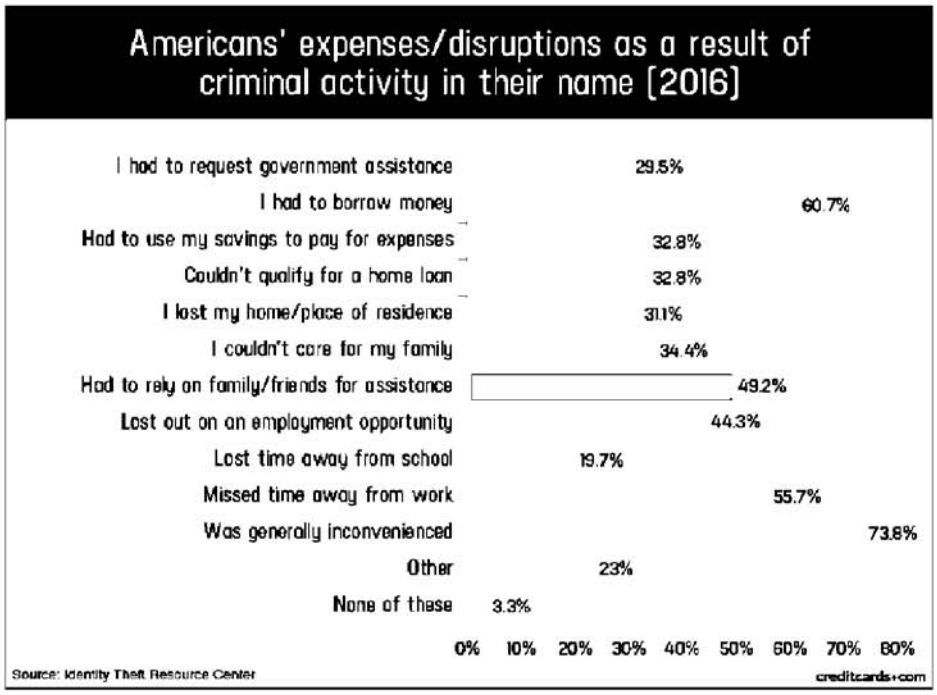
Identity thieves use stolen personal information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. Compl. ¶ 26. Identity thieves can also use SSNs to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and SSN to obtain government

---

[2] Compl. ¶ 24, citing "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," pg. 2, by U.S. Government Accountability Office, June 2007, at: https://www.gao.gov/new.items/d07737.pdf (last visited May 20, 2020) ("GAO Report").

[3] *Id.* ¶ 22, citing https://www.identitytheft.gov/Steps (last visited May 20, 2020).

benefits; or file a fraudulent tax return using the victim's information. *Id.* ¶ 27. In addition, identity thieves may obtain a job using the victim's SSN, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. *Id.* A study by the Identity Theft Resource Center show the multitude of harms caused by fraudulent use of personal and financial information:



Compl. ¶ 28, citing "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/17, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited May 20, 2020).

Personal and financial information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. Compl. ¶ 30. Thus, there is a strong probability that entire batches of

stolen information have been dumped on the black market, and are yet to be dumped on the black market, meaning Plaintiffs and Class members are at an increased risk of fraud and identity theft for many years into the future. *Id.* ¶ 31.

Data breaches are preventable.[4] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[5] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[6] "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[7]

C. As a Result of the Data Breach, Plaintiffs' and Class Members' Personal and Financial Information has been Compromised and Identity Theft has Occurred.

As a result of the Data Breach, Plaintiffs' and Class members' personal information, including their names, Social Security numbers, and street addresses, was compromised and exposed to unauthorized third parties. *See* Notice. Plaintiffs and the Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. *See* Compl. ¶ 80. In addition to fraudulent charges, loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts, and

---

[4] Compl. ¶ 32, citing Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[5] Compl. ¶ 32.
[6] *Id.*
[7] *Id.*

damage to their credit, many victims suffer ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. *Id.* ¶ 81.

Further, despite the Notice saying that there is no indication that the personal information was improperly used, the personal information has *already* been used for identity theft. *See, e.g.*, Compl. ¶¶ 57-69.

1. Plaintiff Bernadette Nolen.

Nolen filed an application for PUA. *See* Affidavit of Bernadette Nolen in Support of Plaintiffs' Emergency Motion for a Temporary Restraining Order ("Nolen Affidavit"), attached hereto as **Exhibit C**, ¶ 2. She received the Notice of the Data Breach on or about May 20, 2020. *Id.* ¶ 3. On May 22, 2020, Nolen received PUA funds and they were directly deposited into her Netspend account, where she had requested the money be deposited. *Id.* ¶ 4. On May 23, 2020, Nolen received a text alert from Netspend stating that her card was reported stolen. *Id.* ¶ 5. She had her card with her at the time and had not reported it stolen. *Id.* ¶ 6.

Nolen immediately called Netspend and the representative stated that her account was locked and her card had been canceled. *Id.* ¶ 7. She was told that a new card would be sent to her in one week, and she would be without access to much needed funds in the meantime. *Id.* ¶ 7. A few hours later, Nolen received an e-mail from Netspend notifying her of a transfer of a substantial amount of money from her supposedly locked account to another account. *Id.* ¶ 8. Nolen had only one authorized account at the time—the account the money was transferred from—and she did not authorize the transfer reported in the e-mail and did not own the account the money was being transferred to. *Id.*

Nolen immediately called Netspend to dispute the transfer and spent approximately an hour and a half on the phone with a Netspend representative attempting to understand what occurred, explain her predicament, and rectify the situation. *Id.* ¶ 9. During this phone call, she was told Netspend had three accounts in her name. *Id.* The dispute is currently pending an internal investigation that could take months to resolve, according to Netspend. *Id.*

In addition, Nolen was notified that a substantial sum of money was wired by Western Union from her authorized Netspend account. *Id.* ¶ 10. She immediately called a Western Union representative but was unable to get very far. *Id.* The representative required a reference number to proceed that Nolen did not have. *Id.* Nolen disputed the charge, and the dispute is currently pending Western Union investigation. *Id.*

On May 24, 2020, Nolen again spoke with a Netspend representative and she was informed that an unauthorized person was attempting to order new cards associated with her Netspend account. *Id.* ¶ 11. In addition, Nolen was notified that her phone account was switched from her Boostmobile account to Metro using her personally identifiable information. *Id.* ¶ 12. Nolen did not authorize the switch. *Id.* She now has a new phone, and the phone is not in her name for her protection. *Id.*

Nolen spent time and effort to file a police report relating to these events for her protection and to secure her information going forward. *Id.* ¶ 13. While the significant issues with her funds are being disputed, she is deprived of urgently needed money to provide for her children's basic needs, including healthcare, as well as her own. *Id.*

2. Plaintiff Nicole Hornbeck.

On May 12, 2020, Hornbeck filed an application for PUA. *See* Affidavit of Marc E. Dann in Support of Plaintiffs' Emergency Motion Pursuant to Civ. R. 65 for a Temporary Restraining Order and/or Preliminary Injunction, attached hereto as **Exhibit D**, with

1 (unsigned Affidavit of Nicole Hornbeck ("Hornbeck Affidavit")), ¶ 2. She elected to receive her benefits by direct deposit to her Netspend bank account ("Account"). *See* Hornbeck Affidavit ¶ 2. On May 20, 2020, she received an email notifying her that her personal and financial information was exposed in the Data Breach. *Id.* ¶ 3.

On May 21, 2020, Hornbeck received her PUA benefits, which were directly deposited in the Account. *Id.* ¶ 4. Later that day, she received an alert from Netspend that her bank card linked to the Account was reported stolen. *Id.* ¶ 5. She knew it was not physically stolen, because she had it in her possession. *Id.* She immediately attempted to login to her bank account online, but her login credentials would not provide her access to her Account. *Id.* ¶ 6.

Hornbeck called the bank, as she was concerned about the security of her Account. *Id.* ¶ 7. She provided her credentials and correctly answered the security questions, reset her credentials, and ordered a new bank card to be delivered to replace the now canceled card. *Id.* She was without the use of the card until the canceled card would be replaced. *Id.*

The next day, on May 22, 2020, she discovered that, using the updated account information, she was again locked out of her account. *Id.* ¶ 8. In a follow up conversation with a Netspend representative, Netspend informed her that, after ten years of banking with Netspend, Netspend decided to end its banking relationship with her. *Id.* ¶ 9. Netspend informed her that it would send by mail a check for the money in her account that would reach her in 7¬10 business days. *Id.* Until she receives the check, she will not have access to the money in her account,

which is her primary account for making purchases, and which includes the much-needed PUA benefits. *Id.*

In addition, Hornbeck received two alerts from her phone company, Boostmobile, that the pin on her account was requested. *Id.* ¶ 10. She had not requested the pin, nor authorized another person to do so. *Id.* She made a phone call to Boostmobile to inquire, and to ensure the account was secure. *Id.*

II. LEGAL BASIS FOR INJUNCTIVE RELIEF.

"[T]he primary purpose of preliminary injunctive relief is to preserve the status quo pending final determination of the matter." *CS/RW Westlake Indoor Storage, L.L.C. v. Russo*, 8th Dist., Cuyahoga Cty., 2016-Ohio-2845, ¶ 23 (citing *Garono v. State,* 37 Ohio St.3d 171 (1988)). "A court issues a temporary injunction when it is necessary to preserve the status quo of the case to prevent any actions of the parties from making null and unenforceable a final judgment." *Id. (citing Gries Sports Ents., Inc. v. Cleveland Browns Football Co.,* 26 Ohio St.3d 15 (1986)); *see* also R.C. 2727.02 ("A temporary order may be granted restraining an act when it appears by the petition that the plaintiff is entitled to the relief demanded, and such relief, or any part of it, consists in restraining the commission or continuance of such act, the commission or continuance of which, during the litigation, would produce great or irreparable injury to the plaintiff, or when, during the litigation, it appears that the defendant is doing, threatens or is about to do, or is procuring or permitting to be done, such act in violation of the plaintiff's rights respecting the subject of the action, and tending to render the judgment ineffectual.").

"The status quo to be preserved by a preliminary injunction is the last, actual, peaceable, uncontested status which preceded the pending controversy." *Lamar Advantage GP Co., LLC v. City of Cincinnati*, 114 N.E.3d 805, 813 (Ohio Com. Pl. 2018) (citations omitted).

This Motion is brought on an emergency basis to preserve the status quo, by requiring Deloitte to secure the personal and financial information of Plaintiffs and other Pandemic Unemployment Assistance applicants in Defendant's possession, custody, or control to prevent unauthorized access to it

Plaintiffs are entitled to a temporary restraining order ("TRO") and a preliminary injunction because: "(1) there is a substantial likelihood that the plaintiffs will prevail on the merits, (2) the plaintiffs will suffer irreparable injury if the injunction is not granted, (3) no third parties will be unjustifiably harmed if the injunction is granted, and (4) the public interest will be served by the injunction." *Vineyard Fellowship v. Anderson*, 10th Dist., Franklin County, 2015-Ohio-5083, ¶ 11 (Ohio Ct. App. 2015) (quoting *Procter & Gamble Co. v. Stoneham,* 1st Dist., Hamilton County, 140 Ohio App.3d 260, 267 (2000)).

In determining whether to grant injunctive relief, courts have recognized that no one factor is dispositive and that the four factors must be balanced with the "flexibility which traditionally has characterized the law of equity." *Lamar Advantage GP Co., LLC*, 114 N.E.3d at 814; *see also Connor Grp. v. Raney*, 2nd Dist., Montgomery County, 2016-Ohio-2959, ¶ 19; *see also Life Line Screening of Am., Ltd. v. Calger*, 2006-Ohio-7322, ¶ 20, 881 N.E.2d 932, 939–40 (Ohio Com. Pl. 2006).

In the case at hand, all of the elements for injunctive relief are met.

A. Substantial Likelihood that Plaintiffs will Prevail on the Merits.

Plaintiffs can demonstrate a likelihood of success on the merits of the underlying action. The Notice (discussed above) includes language which indicates Deloitte recognizes it has at least some liability, as it states that "We apologize for any concerns or inconvenience as a result of this unauthorized incident. Please be assured that we take very seriously our responsibility to safeguard the personal information you entrust to our care, and deeply regret that this incident occurred." *See* Notice, pp. 1-2.

While Plaintiffs have alleged three separate theories for recovery in this lawsuit, (1) Negligence; (2) Invasion of Privacy; and (3) Injunctive Relief, all of these theories stem from the same facts—that Defendant's actions and inactions resulted in the Data Breach. While it is possible that Plaintiffs may not prevail under every theory of liability at trial, given that Defendant admits that Plaintiffs' and Class members' personal and financial information was unsecured and apologized, it is highly likely that Plaintiffs will prevail on at least some of the theories which they have pled. That is all that is necessary to weigh in favor of granting a temporary restraining order and/or preliminary injunction.

B. Irreparable Harm Will Occur If a TRO/Preliminary Injunction is Not Granted.

Irreparable injury or harm, which must be shown for injunctive relief, "is defined as an injury 'for the redress of which, after its occurrence, there could be no plain, adequate and complete remedy at law, and for which restitution in specie (money) would be impossible, difficult or incomplete.'" *Connor Grp. v. Raney*, 2nd Dist., Montgomery County, 2016-Ohio-2959, ¶ 21 (citing *Dimension Serv. Corp. v. First Colonial Ins. Co.,* 10th Dist. Franklin No. 14AP–368, 2014–Ohio–5108, ¶ 12). "Under Ohio law, a moving party need not demonstrate evidence of actual harm, as a threat is a sufficient basis on which to grant injunctive relief." *Life*

Line Screening of Am., Ltd. v. Calger, 2006-Ohio-7322, ¶ 43, 145 Ohio Misc. 2d 6, 23, 881 N.E.2d 932, 945 (Ohio Com Pl.) (citing *Procter & Gamble Co. v. Stoneham*, 140 Ohio App.3d at 274, 747 N.E.2d 268).

What a plaintiff must show as to the degree of irreparable harm varies inversely with what the plaintiff demonstrates as to its likelihood of success on the merits. *Connor Grp. v. Raney*, 2nd Dist. Montgomery County, 2016-Ohio-2959, ¶ 22 (citing cases). In other words, when there is a strong likelihood of success on the merits, preliminary injunctive relief may be justified even though the plaintiff's case of irreparable injury may be weak and, conversely, where the plaintiff's chance of success on the merits of the claim is low, there generally must be a high likelihood of irreparable harm to justify injunctive relief. *Id.*

By Defendant's own admission, Plaintiffs and Class members have already suffered the disclosure of their personal and financial information as a result of the Data Breach. Defendant's ongoing and continuing wrongful conduct, including its failures to employ reasonably adequate security over Plaintiffs' and Class members' personal and financial information and failures to adequately remedy the effects of the Data Breach, has caused and will continue to cause Plaintiffs and Class members to suffer irreparable harm, including but not limited to: fraudulent charges, fraudulent activity relating to opening new accounts for credit, loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts, damage to their credit, out-of-pocket expenses, the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses. Compl. ¶ 110. Plaintiffs and other PUA applicants are among the most needy during this difficult economic time and they will be irreparably

harmed without a TRO/preliminary injunction because the unauthorized access to their personal and financial information is interfering with their access to funds for basic necessities, such as food, rent, etc. *See, e.g.,* Sections I.C.1 and I.C.2, *supra*.

Moreover, to the extent that Defendant stores on unsecure and unencrypted systems additional personal and financial information of Plaintiffs and Class members that has not already been compromised, further irreparable harm to Plaintiffs and Class members is imminent until such time as Defendant adequately secures the personal and financial information of Plaintiffs and other PUA applicants in Defendant's possession, custody, or control to prevent unauthorized access to it. Plaintiffs and Class members are subject to irreparable injury in the form of identity theft and misuse of their personal and financial information by unauthorized persons.

C. No Undue Hardship is Imposed on Defendant or Others.

It cannot reasonably be argued that an undue hardship will be imposed on Defendant or others by the granting of a TRO/preliminary injunction. The sole impact of a TRO/preliminary injunction will be to prevent irreparable harm to Plaintiffs and Class members by the exposure of their personal and financial information. Plaintiffs seek only to have Deloitte secure this personal and financial information to prevent unauthorized access to it. The requested injunction would do nothing more than preserve the status quo as it existed prior to the Data Breach—*i.e.*, the last, actual, peaceable, uncontested status which preceded the pending controversy—and would not in any way increase the potential liability for Defendant, which weighs in favor of granting the TRO/Preliminary Injunction.

D. The Public Interest Will be Served by Issuing a TRO/Preliminary Injunction.

The public interest is served by the issuance of a TRO/preliminary injunction. The public has an interest in protecting citizens' rights to privacy and preventing the disclosure of citizens' non-public, personal and financial information to unauthorized parties, which can lead to identity theft. Further, it is in the public interest that Plaintiffs and other PUA applicants who are suffering during this pandemic have their personal and financial information secure to prevent interference with their access to funds for their basic necessities.

III. THE COURT, IN ITS DISCRETION, MAY DISPOSE OF THE BOND REQUIREMENT BEFORE ENTERING A TRO/PRELIMINARY INJUNCTION.

"While Ohio R. Civ. P. 65(C) appears to require the fixing of a bond in order to effectuate a preliminary injunction, state courts have followed the lead of federal courts holding that the setting of the amount of an injunctive bond is within the discretion of the court and this includes the discretion to require no bond at all." *Lamar Advantage GP Co., LLC v. City of Cincinnati*, 114 N.E.3d 805, 831 (Ohio Com. Pl. 2018) (citing *Vanguard Transp. Sys., Inc. v. Edwards Transfer & Storage Co., Gen. Commodities Div.*, 109 Ohio App.3d 786, 793, 673 N.E.2d 182 (10th Dist. 1996); *Connor Group v. Raney*, 2016-Ohio-2959, 2016 WL 2841190, ¶¶ 64-66 (2d Dist.); *Colquett v. Byrd*, 59 Ohio Misc. 45, 49, 392 N.E.2d 1328 (Mansfield Muni. 1979); *see also, e.g.*, *Johnson v. Couturier*, 572 F.3d 1067, 1086 (9th Cir. 2009) ("Rule 65(c) invests the district court with discretion as to the amount of security required, if any").

In this instance, there is a good cause for this court to exercise its discretion and issue the TRO/preliminary injunction in the absence of a bond. By filing this Motion, Plaintiffs are asking the court for exceedingly modest relief: an Order obligating Deloitte to do what it was originally supposed to do, that is to secure the personal and financial information of Plaintiffs and other PUA applicants. Additionally, a bond would serve no purpose in this case because granting a

preliminary injunction would not cause Deloitte to sustain any damages by requiring it to secure and encrypt the personal and financial information of Plaintiffs and PUA applicants, as Deloitte already has a duty to protect such information.

Therefore, in light of the foregoing, Plaintiffs have demonstrated good cause for the court to issue a TRO/preliminary injunction.

RELIEF REQUESTED

WHEREFORE, Plaintiffs request that the court enter judgment against Defendant, as follows:

A. Mandatorily enjoin Defendant to secure the personal and financial information of Plaintiffs and other Pandemic Unemployment Assistance applicants in Defendant's possession, custody, or control, to prevent unauthorized access to it;

B. Award Plaintiffs their costs, and attorney fees; and

C. Grant any other relief as is deemed just and proper.

(*See* draft Temporary Restraining Order, attached hereto).

Respectfully submitted,

/s/ Marc Dann
Marc E. Dann (0039425)
Brian D. Flick (0081605)
DANNLAW
P.O. Box 6031040
Cleveland, Ohio 44103
(216) 373-0539 telephone
(216) 373-0536 facsimile
notices@dannlaw.com

Thomas A. Zimmerman, Jr. (*pro hac vice* anticipated)
tom@attorneyzim.com
ZIMMERMAN LAW OFFICES, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602

(312) 440-0020 telephone
(312) 440-4180 facsimile
firm@attorneyzim.com
www.attorneyzim.com

Counsel for Plaintiffs and the putative Class

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing *Plaintiffs' Emergency Motion for Temporary Restraining Order, Exhibits A-D, and Exhibit E - Proposed Entry* was electronically filed with the Cuyahoga County Court of Common Pleas on May 28, 2020 and served upon the following parties via electronic mail at the address listed below:

Daniel Warren, Esq. at dwarren@bakerlaw.com
Baker & Hostettler LLP
127 Public Square, Suite 200
Cleveland, OH 44114
Counsel for Defendant Deloitte Consulting LLP

/s/ Marc Dann
Marc E. Dann (0039425)
Brian D. Flick (0081605)
DANNLAW
Counsel for Plaintiffs and the putative Class

NAILAH K. BYRD
CUYAHOGA COUNTY CLERK OF COURTS
1200 Ontario Street
Cleveland, Ohio 44113

Court of Common Pleas

AMENDED COMPLAINT $75
May 28, 2020 09:05

By: MARC E. DANN 0039425

Confirmation Nbr. 2004283

DANIEL BOZIN, ET AL.

vs.

DELOITTE CONSULTING LLP

CV 20 932778

Judge: DAVID T. MATIA

Pages Filed: 29

EXHIBIT A

IN THE COURT OF COMMON PLEAS
CUYAHOGA COUNTY, OHIO

DANIEL BOZIN, individually and on behalf of all others similarly situated, *et al.* Plaintiffs, v. DELOITTE CONSULTING LLP Defendant.	Case No. CV-20-932778 Judge David T. Matia **FIRST AMENDED CLASS ACTION COMPLAINT FOR DAMAGES** **JURY TRIAL DEMANDED**

Plaintiffs DANIEL BOZIN ("Bozin"), TIMOTHY SMITH ("Smith"), ALEXANDRIA POLICHENA ("Polichena"), BERNADETTE NOLEN ("Nolen"), and NICOLE HORNBECK ("Hornbeck") (collectively, "Plaintiffs"), by and through their attorneys, bring this class action lawsuit on behalf of themselves and all other persons similarly situated, and for their FIRST AMENDED Class Action Complaint against Defendant DELOITTE CONSULTING LLP ("Deloitte" or "Defendant"), Plaintiffs allege with personal knowledge with respect to themselves individually and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters, as follows:

PARTIES

1. Plaintiff DANIEL BOZIN is a natural person with a principal place of residence located in Cuyahoga County, Ohio.

2. Plaintiff TIMOTHY SMITH is a natural person with a principal place of residence in Franklin County, Ohio.

3. Plaintiff ALEXANDRIA POLICHENA is a natural person with a principal place of residence in Portage County, Ohio.

4. Plaintiff BERNADETTE NOLEN is a natural person with a principal place of residence in Trumbull County, Ohio.

5. Plaintiff NICOLE HORNBECK is a natural person with a principal place of residence in Franklin County, Ohio.

6. Defendant DELOITTE CONSULTING LLP is a Delaware limited liability company with a principal place of business in Hermitage, TN.

7. Venue lies in this Court pursuant to Civ. R. 3(B) as a substantial portion of the events that form the basis of this Class Action Complaint occurred in Cuyahoga County, Ohio; Defendant conducted activity that gave rise to the claims for relief in this County; and Defendant maintains an office in this County.

THE DATA BREACH

8. Plaintiffs bring this suit on behalf of themselves and a Class of similarly situated individuals against Defendant for Defendant's failure to secure and protect Plaintiffs' and Class members' personal and financial information.

9. At one of the worst times in the lives of Plaintiffs and Class members, when they find themselves unemployed in the midst of a pandemic and resulting recession, Deloitte was brought in as an expert consultant by certain states, including Colorado, Illinois, and Ohio, to facilitate the secure and efficient processing of Plaintiffs' and Class members' claims for Pandemic Unemployment Assistance ("PUA"). However, Deloitte negligently and recklessly made the Plaintiffs' and Class members' path to recovery significantly harder by putting their

identity and credit standing at risk.

10. On May 20, 2020, Bozin received an email, which is attached as Exhibit 1 to this Complaint (the "Notice").

11. The Notice stated:

> Dear PUA Applicant:
>
> Deloitte Consulting is currently under contract with the Ohio Department of Job and Family Services (ODJFS) to assist the state of Ohio in administering the Pandemic Unemployment Assistance (PUA) program. Deloitte discovered on May 15, 2020 that your name, Social Security number, and street address pertaining to your application for and receipt of unemployment compensation benefits inadvertently had the capability to be viewed by other unemployment claimants. Thereafter, Deloitte immediately began an investigation and upon discovering the exposure, Deloitte immediately took steps to stop further access to and exposure of your personal information.
>
> At this time, there is no evidence or indication to believe that your personal information was improperly used; therefore, our actions, as well as the actions you may want to consider, are preventative.
>
> As a precaution, you may want to monitor your credit by obtaining a copy of your credit report from one of the three national credit bureaus. Federal law entitles every individual to one free credit report per year from each of the three main bureaus.
>
> You may also have a fraud alert placed on your consumer credit file by contacting one of the national credit bureaus. Once one credit bureau places a fraud alert on your credit file, it notifies the other two bureaus. Fraud alerts are typically in effect for 90 days but can be renewed. The credit bureaus may be contacted at:
>
> Equifax: (800) 525-6285 (http://www.equifax.com)
> Experian: (888) 397-3742 (http://www.experian.com)
> TransUnion: (800) 680-7289 (http://www.tuc.com)

> Additionally, Ohio law allows you to place a security freeze on your credit report by contacting one of the bureaus listed above. Should you wish to open a new line of credit while your report is frozen, you may temporarily lift this security freeze by telephone or online by providing a security code. Credit reporting agencies may charge a fee of no more than $5 for each freeze and unfreeze of your report.
>
> If you wish to receive free Experian IdentityWorks identity protection services for the next 12 months, you will receive a follow-up email with enrollment details that will be sent to you via Deloitte or directly from Experian within 3-5 days.
>
> Finally, to find out more about protecting your personal information, visit the Ohio Attorney General's Identity Theft protection page (http://www.ohioattorneygeneral.gov/IdentityTheft) and/or the Federal Trade Commission's identity theft assistance page (https://www.consumer.ftc.gov/features/feature-0014-identitytheft).
> We apologize for any concerns or inconvenience as a result of this unauthorized incident. Please be assured that we take very seriously our responsibility to safeguard the personal information you entrust to our care, and deeply regret that this incident occurred.
>
> If you have questions or concerns that remain unaddressed after reviewing this information, please email:
> DeloitteIdentityhelp@jfs.ohio.gov.

See Exhibit 1 at pp. 1-2.

12. On May 20, 2020, the same Notice was sent to Smith via e-mail.

13. On May 20, 2020, the same Notice was sent to Polichena via e-mail.

14. On May 20, 2020, the same Notice was sent to Nolen via e-mail.

15. On May 20,2020, the same Notice was sent to Hornbeck via e-mail.

16. The Notice acknowledges that a treasure trove of highly sensitive personal information was subject to unauthorized access by numerous third parties (the "Data Breach").

See Exhibit 1 at p. 1.

17. As a result of the Data Breach, Plaintiffs and Class members must now be vigilant and review their credit reports for incidents of identity theft, and to educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft.

18. Data security breaches have dominated the headlines for the last two decades, and it does not take an IT industry expert to know that major businesses who fail to take reasonable security precautions like Deloitte are at risk.

19. The general public can tell you the names of some of the biggest data breaches: LabCorp, Quest Diagnostics, Yahoo, Equifax, Marriott International, Target, Home Depot, Anthem, Heartland Payment Systems, and TJX Companies, Inc.[1]

20. Deloitte is no stranger to data breaches and phishing scams of its own employees.[2]

21. Upon information and belief, Deloitte failed to implement reasonable industry standards necessary to prevent a data breach, including the FTC's guidelines, resulting in the Data Breach.

22. Likewise, Deloitte failed to create, maintain, and/or comply with a written cybersecurity program that incorporated physical, technical, and administrative safeguards for the protection of personal information and reasonably conformed to an industry recognized cybersecurity framework, resulting in the Data Breach.

---

[1] S*ee, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[2] *See, e.g., Source: Deloitte Breach Affected All Company Email, Admin Accounts*, Krebsonsecurity.com (September 25, 2017) (last visited May 20, 2020) https://krebsonsecurity.com/2017/09/source-deloitte-breach-affected-all-company-email-admin-accounts/

23. Because of its failure to create, maintain, and/or comply with a necessary cybersecurity program, Deloitte was unable to ensure the protection of information security and confidentiality, and protect against obvious and readily foreseeable threats to information security and confidentiality or the unauthorized access to the personal and financial information, resulting in the Data Breach.

DAMAGES FROM DATA BREACHES

24. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[3]

25. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[4]

26. Identity thieves use stolen personal information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

27. Identity thieves can also use SSNs to obtain a driver's license or official

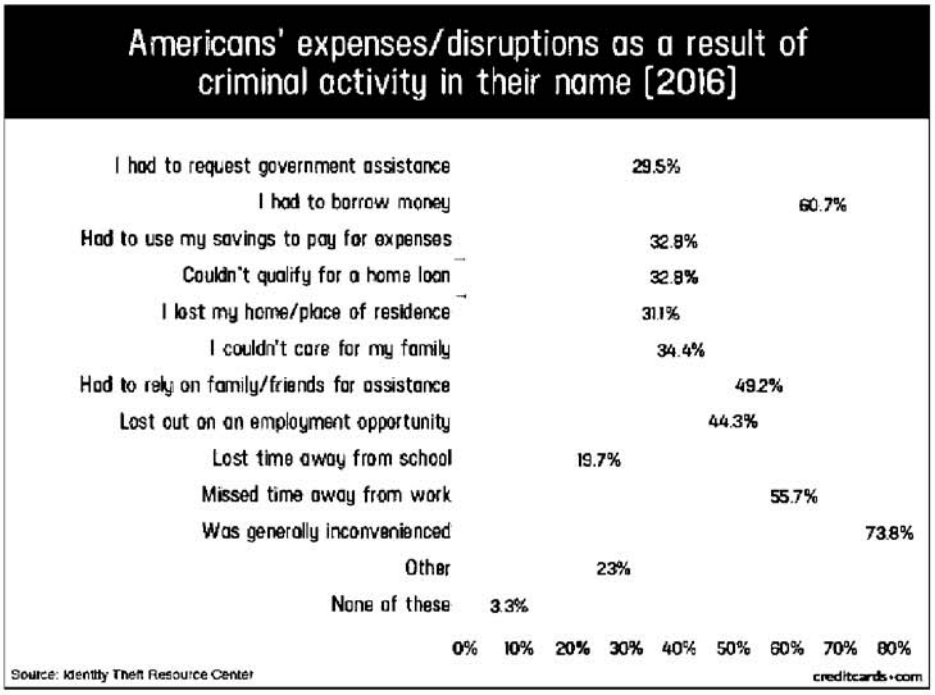
---

[3] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," pg. 2, by U.S. Government Accountability Office, June 2007, at: https://www.gao.gov/new.items/d07737.pdf (last visited May 20, 2020) ("GAO Report").

[4] *See* https://www.identitytheft.gov/Steps (last visited May 20, 2020).

identification card in the victim's name but with the thief's picture; use the victim's name and SSN to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

28. A study by the Identity Theft Resource Center show the multitude of harms caused by fraudulent use of personal and financial information:



Source: "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/17, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited May 20, 2020).

29. There may be a time lag between when harm occurs versus when it is discovered, and also between when personal and financial information is stolen and when it is used.

According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

30. Personal and financial information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

31. Thus, there is a strong probability that entire batches of stolen information have been dumped on the black market, and are yet to be dumped on the black market, meaning Plaintiffs and Class members are at an increased risk of fraud and identity theft for many years into the future.

32. Data breaches are preventable.[5] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[6] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[7]

---

[5]Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[6]*Id.* at 17.
[7]*Id.* at 28.

33. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[8]

FACTS RELEVANT TO PLAINTIFF DANIEL BOZIN

34. Bozin is a citizen of Ohio (and was during the period of the Data Breach).

35. On May 13, 2020, Bozin applied online with the Ohio Department of Job and Family Services ("ODJFS") for pandemic unemployment assistance ("PUA").

36. At the time Bozin applied online for PUA, the website was being operated by Deloitte.

37. Shortly after he applied for benefits on May 13, 2020, Bozin emailed ODJFS through the website to request his application be cancelled, as he discovered he was eligible to receive unemployment benefits, along with PUA, in another state.

38. On May 15, 2020, Bozin emailed ODJFS through the website to follow up on his request.

39. On May 20, 2020, Bozin received the Notice.

40. Shortly after receiving the Notice, Bozin was concerned that his identity may have been stolen. Therefore, he purchased credit and identity monitoring software with Lifelock.

41. As a direct result of the Data Breach, Bozin will now have to expend additional time and energy reviewing alerts from Lifelock, verifying his identity with potential creditors, and monitoring his credit, in addition to the monthly service fee he is now paying.

---

[8] *Id.*

42. Bozin also intends to close financial accounts in the event that these accounts are actually compromised as a result of the Data Breach.

FACTS RELEVANT TO PLAINTIFF TIMOTHY SMITH

43. Smith is a citizen of Ohio (and was during the period of the Data Breach).

44. On May 12, 2020, Smith applied online with the ODJFS for PUA.

45. At the time Smith applied online for PUA, the website was being operated by Deloitte.

46. On May 20, 2020, Smith received the Notice.

47. Shortly after receiving the Notice, Smith was concerned that his identity may have been stolen. Therefore, he purchased credit and identity monitoring software with Lifelock.

48. As a direct result of the Data Breach, Smith will now have to expend additional time and energy reviewing alerts from Lifelock, verifying his identity with potential creditors, and monitoring his credit, in addition to the monthly service fee he is now paying.

49. Smith also intends to close financial accounts in the event that these accounts are actually compromised as a result of the Data Breach.

FACTS RELEVANT TO PLAINTIFF ALEXANDRIA POLICHENA

50. Polichena is a citizen of Ohio (and was during the period of the Data Breach).

51. Prior to May 15, 2020, Polichena applied online with the ODJFS for PUA.

52. At the time Polichena applied online for PUA, the website was being operated by Deloitte.

53. On May 20, 2020, Polichena received the Notice.

54. Shortly after receiving the Notice, Polichena was concerned that her identity may have been stolen. Therefore, she purchased credit and identity monitoring software with Lifelock.

55. As a direct result of the Data Breach, Polichena will now have to expend additional time and energy reviewing alerts from Lifelock, verifying her identity with potential creditors, and monitoring her credit, in addition to the monthly service fee she is now paying.

56. Polichena also intends to close financial accounts in the event that these accounts are actually compromised as a result of the Data Breach.

FACTS RELEVANT TO PLAINTIFF BERNADETTE NOLEN

57. Nolen is a citizen of Ohio (and was during the period of the Data Breach).

58. At the time Nolen applied online with the ODJFS, the website was being operated by Deloitte.

59. On or around May 20, 2020, Nolen received the Notice.

60. On May 22, 2020, Nolen received PUA funds and they were directly deposited into her Netspend account, where she had requested the money be deposited.

61. On May 23, 2020, Nolen received a text alert from Netspend stating that her card was reported stolen.

62. Nolen had her card with her at the time she received the text alert from Netspend, and she had not reported it stolen.

63. Nolen immediately called Netspend and the representative stated that her account was locked and her card had been canceled. Nolen was told that a new card would be sent to her in one week, and she would be without access to much needed funds in the meantime.

64. A few hours later, Nolen received an e-mail from Netspend notifying her of a transfer of a substantial amount of money from her supposedly locked account to another account. Nolen had only one authorized account at the time—the account the money was transferred from—and she did not authorize the transfer reported in the e-mail and did not own the account the money was being transferred to.

65. Nolen immediately called Netspend to dispute the transfer, and she spent approximately an hour and a half on the phone with a Netspend representative attempting to understand what occurred, explain her predicament, and rectify the situation. During this phone call, she was told Netspend had three accounts in her name. The dispute is currently pending an internal investigation that could take months to resolve, according to Netspend.

66. In addition, Nolen was notified that a substantial sum of money was wired by Western Union from her Netspend account. She immediately called a Western Union representative but was unable to get very far. The representative required a reference number to proceed that Nolen did not have. Nolen disputed the charge, and the dispute is currently pending Western Union's investigation.

67. On May 24, 2020, Nolen again spoke with a Netspend representative and she was informed that an unauthorized person was attempting to order new cards associated with her Netspend account.

68. In addition, Nolen was notified that her phone account was switched from her Boostmobile account to Metro using her personal and financial information. Nolen did not authorize the switch. She now has a new phone, and the phone is not in her name for her protection.

69. Nolen spent time and effort to file a police report relating to these events for her protection and to secure her information going forward. While the significant issues with Nolen's funds are being disputed, Nolen is deprived of urgently needed money to provide for her childrens' basic needs, including healthcare, as well as her own.

FACTS RELEVANT TO PLAINTIFF NICOLE HORNBECK

70. Hornbeck is a citizen of Ohio (and was during the period of the Data Breach).

71. On May 12, 2020, Hornbeck filed an application for PUA. She elected to receive her benefits by direct deposit to her Netspend bank account.

72. On May 20, 2020, Hornbeck received an email notifying her that her personal and financial information was exposed in the Data Breach.

73. On May 21, 2020, Hornbeck received her PUA benefits, which were directly deposited in her Netspend account.

74. Later that day, Hornbeck received an alert from Netspend that her bank card was reported stolen. Hornbeck knew it was not physically stolen, because she had it in her possession.

75. Hornbeck immediately attempted to login to her bank account, but her login credentials would not provide her access to her account.

76. Hornbeck called her bank concerned about the security of her account. She provided her credentials and correctly answered the security questions, reset her credentials, and ordered a new bank card to be delivered to replace her now canceled card. She was without the use of her card until her canceled card would be replaced.

77. The next day, on May 22, 2020, Hornbeck discovered that, using her updated account information, she was again locked out of her account.

78. In a follow up conversation with a Netspend representative, Netspend informed Hornbeck that, after ten years of banking with Netspend, Netspend decided to end their banking relationship. Netspend informed Hornbeck that it would send by mail a check for the money in her account that would reach her in 7–10 business days. Until Hornbeck receives her check, she will not have access to the money in her account, which is her primary account for making purchases, and which includes her much-needed PUA benefits.

79. In addition, Hornbeck received two alerts from her phone company, Boostmobile, that the pin on her account was requested. She had not requested her pin, nor authorized another person to do so. She made a phone call to Boostmobile to inquire and ensure her account was secure.

PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

80. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

81. Plaintiffs and members of the Class have or will suffer actual injury as a direct result of the Data Breach. In addition to fraudulent charges, loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts, and damage to their credit, many victims suffer ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards linked to their bank accounts;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Taking trips to banks and waiting in line to verify their identities in order to restore access to the accounts;

g. Placing "freezes" and "alerts" with credit reporting agencies which, pursuant to ORC 1349.52(I), will cost up to $5.00 per security freeze placed and up to $5.00 per security freeze to be removed;

h. Spending time on the phone with or at the financial institution to dispute fraudulent charges;

i. Contacting their financial institutions and closing or modifying financial accounts;

j. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

k. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

82. Moreover, Plaintiffs and the Class members have an interest in ensuring that their personal and financial information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

83. In the Notice, Plaintiffs and Class members are given minimal information, other

than boilerplate steps that any person can take in the event of a data breach.

84. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class members have suffered anxiety, emotional distress, loss of privacy, financial damages, and are at an increased risk of future harm.

CLASS ALLEGATIONS

85. **Class Definition**: Plaintiffs bring this action pursuant to Fed. R. Civ. P. 23, on behalf of a class of similarly situated individuals and entities ("the Class"), defined as follows:

> All individuals who applied for Pandemic Unemployment Assistance, including with the Colorado Department of Labor and Employment, Illinois Department of Employment Security, and Ohio Department of Job and Family Services, and whose personal information and/or financial information was exposed in the Data Breach.
>
> Excluded from the Class are: (1) Defendant, Defendant's agents, subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest, and those entities' current and former employees, officers, and directors; (2) the Judge to whom this case is assigned and the Judge's immediate family; (3) any person who executes and files a timely request for exclusion from the Class; (4) any persons who have had their claims in this matter finally adjudicated and/or otherwise released; and (5) the legal representatives, successors and assigns of any such excluded person.

86. **Numerosity**: Upon information and belief, the Class is comprised of hundreds of thousands of members. The actual number is unknown at present. Initial reports state that approximately 72,000 Coloradans, 32,500 Illinoisans, and 130,000 Ohioans had sensitive and confidential information exposed.[9] Thus, the Class is so numerous that joinder of all members is

---

[9] *See* https://www.kktv.com/content/news/Colorado-Labor-Department-confirms-brief-data-exposure-for-pandemic-unemployment-claimants-570633261.html; https://www.illinoispolicy.org/state-agency-published-private-data-of-nearly-32500-unemployed-illinoisans/;

impracticable. Class members can easily be identified through Defendant's records, or by other means.

87. **Commonality and Predominance**: There are several questions of law and fact common to the claims of Plaintiffs and Class members, which predominate over any individual issues, including:

a. Whether Defendant adequately protected the personal and financial information of Plaintiffs and members of the Class;

b. Whether Defendant placed the personal and financial information of Plaintiffs and members of the Class in an online storage server without a secure lock on any of the files and was not password-protected;

c. Whether Defendant adopted, implemented, and maintained reasonable policies and procedures to prevent the unauthorized access to the personal and financial information of Plaintiffs and members of the Class;

d. Whether Defendant properly trained and supervised its employees to protect the personal and financial information of Plaintiffs and members of the Class;

e. Whether Defendant promptly notified Plaintiffs and members of the Class of the Data Breach;

f. Whether Defendant owed a duty to Plaintiffs sand members of the Class to safeguard and protect their personal and financial information;

g. Whether Defendant breached a duty to Plaintiffs and members of the Class to safeguard and protect their personal and financial information;

h. Whether Defendant breached a duty to Plaintiffs and members of the Class by failing to adopt, implement, and maintain reasonable policies and procedures to safeguard and protect the personal and financial information of Plaintiffs and members of the Class; and

i. Whether Defendant is liable for the damages suffered by Plaintiffs and members of the Class as a result of the Data Breach.

---

https://www.wlwt.com/article/unemployment-data-system-breach-in-ohio-puts-thousands-of-applicants-info-at-potential-risk/32620720 (last visited May, 22, 2020).

88. **Typicality**: Plaintiffs' claims are typical of the claims of members of the Class. All claims are based on the same legal and factual issues. Plaintiffs and each of the Class members provided their personal and financial information to Deloitte, and the information was placed in an online storage server that did not have a secure lock and was not password-protected. Defendant's conduct was uniform to Plaintiffs and all Class members.

89. **Adequacy of Representation**: Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class, and have retained counsel competent and experienced in complex class actions. Plaintiffs have no interest antagonistic to those of members of the Class, and Defendant has no defenses unique to Plaintiffs. The questions of law and fact common to the proposed Class predominate over any questions affecting only individual members of the Class.

90. **Superiority**: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for proposed members of the Class to prosecute their claims individually. The trial and the litigation of Plaintiffs' claims are manageable.

COUNT I
Negligence
(On behalf of Plaintiffs and the Class)

91. Plaintiffs repeat and reallege the allegations of paragraphs 1-90 with the same force and effect as though fully set forth herein.

92. Deloitte knew, or should have known, of the risks inherent in collecting and storing the personal and financial information of Plaintiffs and Class members and the

importance of adequate security. Deloitte was well aware of numerous, well-publicized data breaches that exposed the personal and financial information of individuals.

93. Deloitte had a common law duty to prevent foreseeable harm to those whose personal and financial information it was entrusted. This duty existed because Plaintiffs and Class members were the foreseeable and probable victims of the failure of Deloitte to adopt, implement, and maintain reasonable security measures so that Plaintiffs' and Class members' personal and financial information would not be accessible in an unsecured online storage server and not password-protected.

94. Deloitte had a special relationship with Plaintiffs and Class members. Deloitte was entrusted with Plaintiffs' and Class members' documents and electronic data containing their personal and financial information, and Deloitte was in a position to protect the documents and electronic data (and the personal and financial information stored on them) from public exposure.

95. The duties of Deloitte also arose under section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect individuals' personal and financial information by companies. Various FTC publications and data security breach orders further form the basis of the duties of Deloitte.

96. Deloitte had a duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiffs' and Class members' personal and financial

information in its possession so that the personal and financial information would not come within the possession, access, or control of unauthorized persons.

97. More specifically, the duties of Deloitte included, among other things, the duty to:

a. Adopt, implement, and maintain policies, procedures, and security measures for protecting documents containing an individual's personal and financial information, including policies, procedures, and security measures to ensure that the documents are not accessible online in unsecured storage servers and are password-protected;

b. Adopt, implement, and maintain reasonable policies and procedures to prevent the sharing of documents containing an individual's personal and financial information with entities that failed to adopt, implement, and maintain policies, procedures, and security measures to ensure that the documents are not accessible online in unsecured storage servers and are password-protected;

c. Adopt, implement, and maintain reasonable policies and procedures to ensure that it is sharing documents containing an individual's personal and financial information only with entities that have adopted, implemented, and maintained policies, procedures, and security measures to ensure that the documents are not accessible online in unsecured storage servers and are password-protected;

d. Properly train its employees to protect documents containing an individual's personal and financial information; and

e. Adopt, implement, and maintain processes to quickly detect a data breach and to promptly act on warnings about data breaches.

98. Deloitte breached the foregoing duties to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the documents and electronic data containing an individual's personal and financial information in its possession so that the documents and electronic data would not come within the possession, access, or control of unauthorized persons. The Notice acknowledges that the personal information of the Plaintiffs and the Class members was exposed in the Data Breach. The experiences of Plaintiffs shows

that their personal and financial information was accessed and misused by unauthorized third parties.

99. Deloitte acted with reckless disregard for the security of the personal and financial information of Plaintiffs and the Class because Deloitte knew or should have known that its data security practices were not adequate to safeguard the personal and financial information that it collected and stored.

100. Deloitte acted with reckless disregard for the rights of Plaintiffs and the Class by failing to promptly detect the Data Breach so that Plaintiffs and the Class members could take measures to protect themselves from damages caused by the unauthorized access of the personal and financial information compromised in the Data Breach.

101. Deloitte's data security violations were so egregious that numerous unauthorized persons were able to—and actually did—easily navigate to Deloitte's website(s), and view, access, download, and disseminate reams of personally identifiable and financially valuable information of tens of thousands of people all at once.

102. At least some of these unauthorized persons were able to—and actually did—transmit and further disseminate the personally identifiable and financially valuable information of tens of thousands of people all at once.

103. As a result of the conduct of Deloitte, Plaintiffs and Class members have suffered and will continue to suffer actual damages including, but not limited to, expenses and/or time spent on credit monitoring; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts; and increased risk of future harm. Further, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury

and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT II
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

104. Plaintiffs repeat and reallege the allegations of paragraphs 1–90 with the same force and effect as though fully set forth herein.

105. Defendant invaded the right to privacy of Plaintiffs and Class members by displaying, disclosing, and allowing unfettered access of their personal and financial information to unauthorized and unknown individuals, and by failing to employ reasonable and necessary safeguards to prevent unauthorized access to Plaintiffs' and Class members' personal and financial information.

106. Plaintiffs' and Class members' personal and financial information was held privately and confidentially by them, and used only for legitimate personal and financial purposes. They only entrusted their personal and financial information with third parties as necessary for legitimate purposes, and required the third parties to hold the personal and financial information in confidence at all times and protect it against unauthorized disclosures. Plaintiffs and Class members were reasonable in expecting Defendant to maintain the security and confidentiality of their personal and financial information.

107. Defendant's conduct was and is highly offensive to a reasonable person with ordinary sensibilities.

108. As a result of the conduct of Deloitte, Plaintiffs and Class members have suffered and will continue to suffer actual damages including, but not limited to, expenses and/or time

spent on credit monitoring; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts; and increased risk of future harm. Further, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT III
Injunctive Relief
(On Behalf of Plaintiffs and the Class)

109. Plaintiffs repeat and reallege the allegations of paragraphs 1–90 with the same force and effect as though fully set forth herein.

110. Defendant's ongoing and continuing wrongful conduct, including its failures to employ reasonably adequate security over Plaintiffs' and Class' members' personal and financial information and failures to adequately remedy the effects of the Data Breach, has caused and will continue to cause Plaintiffs and Class members to suffer irreparable harm, including but not limited to: fraudulent charges, fraudulent activity relating to opening new accounts for credit, loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts, damage to their credit, out-of-pocket expenses, the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

111. Such irreparable harm will not cease unless enjoined by the Court.

112. Plaintiffs and the Class are entitled to injunctive relief and other affirmative equitable relief, including, but not limited to: an order compelling Defendant to: (i) notify each person whose personal and financial information was in Defendant's possession during the Data

Breach; (ii) provide credit monitoring protection for each such person without opting in and at no cost to the person for a reasonable time period exceeding one year; (iii) secure its computer environment containing Plaintiffs' and Class members' personal and financial information, and to implement and continuously employ industry standard and reasonable security procedures for the protection of their personal and financial information; and (iv) require independent third party audits for a reasonable period of time going forward to ensure that Defendant maintains reasonable industry standard data security practices.

113. If the requested injunction is not issued, Plaintiffs and the Class will suffer and continue to suffer irreparable injury in the form of continued exposure of their personal and financial information, further dissemination of their personal and financial information, and identity theft and fraud. In addition, Defendant is subject to another cyber attack now that its insufficient data security practices are known. The threat of a future data breach exposing Plaintiffs' and Class members' personal and financial information is immediate, substantial, and real.

114. The hardship to Plaintiffs and Class members were the injunction not to issue would be significant. Defendant continues to possess and handle Plaintiffs' and Class members' personal and financial information. Plaintiffs and Class members bear the brunt of harm of another data breach, while Defendant does not suffer real loss.

115. The requested injunctive relief is in the public interest, as it will provide assurances and security to Plaintiffs and Class members who are already vulnerable and in need of assistance, and will facilitate the increased participation in the PUA program, which exists for the purpose of aiding Plaintiffs and the Class, as well as future applicants and the economy.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs DANIEL BOZIN, TIMOTHY SMITH, ALEXANDRIA POLICHENA, BERNADETTE NOLEN, and NICOLE HORNBECK, individually, and on behalf of all others similarly situated, respectfully request that judgment be entered in their favor and against DELOITTE CONSULTING LLP, as follows:

A. That the Court find that this action satisfies the prerequisites for maintenance as a class action and certifying the Class defined herein;

B. That the Court appoint Plaintiffs as representatives of the Class;

C. That the Court appoint Plaintiffs' counsel as counsel for the Class;

D. That the Court enter judgment in favor of Plaintiffs and the Class against Deloitte;

E. That the Court award Plaintiffs and Class members actual damages and all other forms of available relief, as applicable;

F. That the Court award Plaintiffs and Class members punitive damages and all other forms of available relief, as applicable;

G. That the Court award Plaintiffs and the Class attorney's fees and costs, including interest thereon as allowed or required by law;

H. That the Court enter an injunction as set forth above, including requiring Deloitte to adopt, implement, and maintain adequate security measures to protect Plaintiffs' and Class members' personal and financial information; and

I. Granting all such further and other relief as the Court deems just and appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs Daniel Bozin, Timothy Smith, Alexandria Polichena, Bernadette Nolen, and Nicole Hornbeck, individually, and on behalf of all others similarly situated, hereby demand a trial by jury of all claims so triable.

Respectfully submitted,

/s/ Marc Dann
Marc E. Dann (0039425)
Brian D. Flick (0081605)
DannLaw
P.O. Box 6031040
Cleveland, Ohio 44103
(216) 373-0539 telephone
(216) 373-0536 facsimile
notices@dannlaw.com

Thomas A. Zimmerman, Jr. (*pro hac vice* anticipated)
tom@attorneyzim.com
Zimmerman Law Offices, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
(312) 440-0020 telephone
(312) 440-4180 facsimile
www.attorneyzim.com

Counsel for Plaintiffs and the putative Class

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing *Plaintiffs' First Amended Class Action Complaint for Damages* was electronically filed with the Cuyahoga County Court of Common Pleas on May 28, 2020 and served upon the following parties via electronic mail at the address listed below:

Daniel Warren, Esq. at dwarren@bakerlaw.com Baker & Hostettler LLP
127 Public Square, Suite 200
Cleveland, OH 44114
Counsel for Defendant Deloitte Consulting LLP

and upon the following party via ordinary first-class mail on May 28, 2020:

Deloitte Consulting LLP
c/o Corporation Servicing Company
50 W. Broad St, Suite 1330
Columbus, OH 43215

/s/ Marc Dann
Marc E. Dann (0039425)
Brian D. Flick (0081605)
DannLaw
Counsel for Plaintiffs and the putative Class

EXHIBIT 1

Dann Law

Brian Flick <bflick@dannlaw.com>

Fwd: Pandemic Unemployment Assistance

1 message

Dan Bozin [redacted]@gmail.com> Wed, May 20, 2020 at 5:56 PM
To: bflick@dannlaw.com

Begin forwarded message:

From: noreply@jfs.ohio.gov
Subject: Pandemic Unemployment Assistance
Date: May 20, 2020 at 2:46:12 PM EDT
To: [redacted]@gmail.com <[redacted]@gmail.com>

May 20, 2020

Dear PUA Applicant:

Deloitte Consulting is currently under contract with the Ohio Department of Job and Family Services (ODJFS) to assist the state of Ohio in administering the Pandemic Unemployment Assistance (PUA) program. Deloitte discovered on May 15, 2020 that your name, Social Security number, and street address pertaining to your application for and receipt of unemployment compensation benefits inadvertently had the capability to be viewed by other unemployment claimants. Thereafter, Deloitte immediately began an investigation and upon discovering the exposure, Deloitte immediately took steps to stop further access to and exposure of your personal information.

At this time, there is no evidence or indication to believe that your personal information was improperly used; therefore, our actions, as well as the actions you may want to consider, are preventative.

As a precaution, you may want to monitor your credit by obtaining a copy of your credit report from one of the three national credit bureaus. Federal law entitles every individual to one free credit report per year from **each** of the three main bureaus.

You may also have a fraud alert placed on your consumer credit file by contacting one of the national credit bureaus. Once one credit bureau places a fraud alert on your credit file, it notifies the other two bureaus. Fraud alerts are typically in effect for 90 days but can be renewed. The credit bureaus may be contacted at:

Equifax: (800) 525-6285 (http://www.equifax.com)
Experian: (888) 397-3742 (http://www.experian.com)
TransUnion: (800) 680-7289 (http://www.tuc.com)

Additionally, Ohio law allows you to place a security freeze on your credit report by contacting one of the bureaus listed above. Should you wish to open a new line of credit while your report is frozen, you may temporarily lift this security freeze by telephone or online by providing a security code. Credit reporting agencies may charge a fee of no more than $5 for each freeze and unfreeze of your report.

If you wish to receive free Experian IdentityWorks identity protection services for the next 12 months, you will receive a follow-up email with enrollment details that will be sent to you via Deloitte or directly from Experian within 3-5 days.

Finally, to find out more about protecting your personal information, visit the Ohio Attorney General's Identity Theft protection page (http://www.ohioattorneygeneral.gov/IdentityTheft) and/or the Federal Trade Commission's identity theft assistance page (https://www.consumer.ftc.gov/features/feature-0014-identity-theft).

We apologize for any concerns or inconvenience as a result of this unauthorized incident. Please be assured that we take very seriously our responsibility to safeguard the personal information you entrust to

our care, and deeply regret that this incident occurred.

If you have questions or concerns that remain unaddressed after reviewing this information, please email: DeloitteIdentityhelp@jfs.ohio.gov.

IN THE COURT OF COMMON PLEAS
CUYAHOGA COUNTY, OHIO

DANIEL BOZIN, individually and on behalf of all others similarly situated, *et al.* Plaintiffs, v. DELOITTE CONSULTING LLP Defendant.	Case No.: CV 20 932778 Judge David T. Matia

AFFIDAVIT OF BRIAN D. FLICK IN SUPPORT OF PLAINTIFFS' EMERGENCY MOTION PURSUANT TO CIV. R. 65 FOR A TEMPORARY RESTRAINING ORDER AND/OR PRELIMINARY INJUNCTION

I, BRIAN D. FLICK, hereby certifies as follows:

1. I am over the age of 18 years. I am competent and willing to testify as to the facts set forth in this Affidavit, which are based on my personal knowledge, unless stated otherwise.

2. On May 23, 2020 DannLaw was contacted by Samantha Smith, a resident of Zanesville, Ohio regarding the Complaint filed in this matter on May 20, 2020.

3. On May 26, 2020 I reviewed the attached postings from a Facebook Group Page titled "Ohio - Pandemic Unemployment Assistance" forwarded via email by Ms. Smith to DannLaw. These postings are attached as **Exhibit 1** to this Affidavit.

4. On May 26, 2020 I independently viewed the Facebook Group Page and Comments sections to verify the postings of **Exhibit 1** were associated with that Page.

5. We will supplement our motion with an affidavit signed by Samantha Smith when she is able to obtain a notarization during the current Covid-19 emergency.

FURTHER SAYETH NAUGHT.

I affirm under the penalties of perjury that the above and foregoing statements and

EXHIBIT B

representations are true and correct.

Executed on this 28th day of May, 2020.

Brian Flick

STATE OF OHIO

ss::

COUNTY OF HAMILTON

Sworn to and subscribed before me, a notary public, this 28 day of May, 2020 by Brian D. Flick, Esq. the Affiant herein.

NOTARY PUBLIC

My Commission Expires:_____

MIKE HARRIS
Notary Public, State of Ohio
My Comm. Expires Sept. 23, 2023

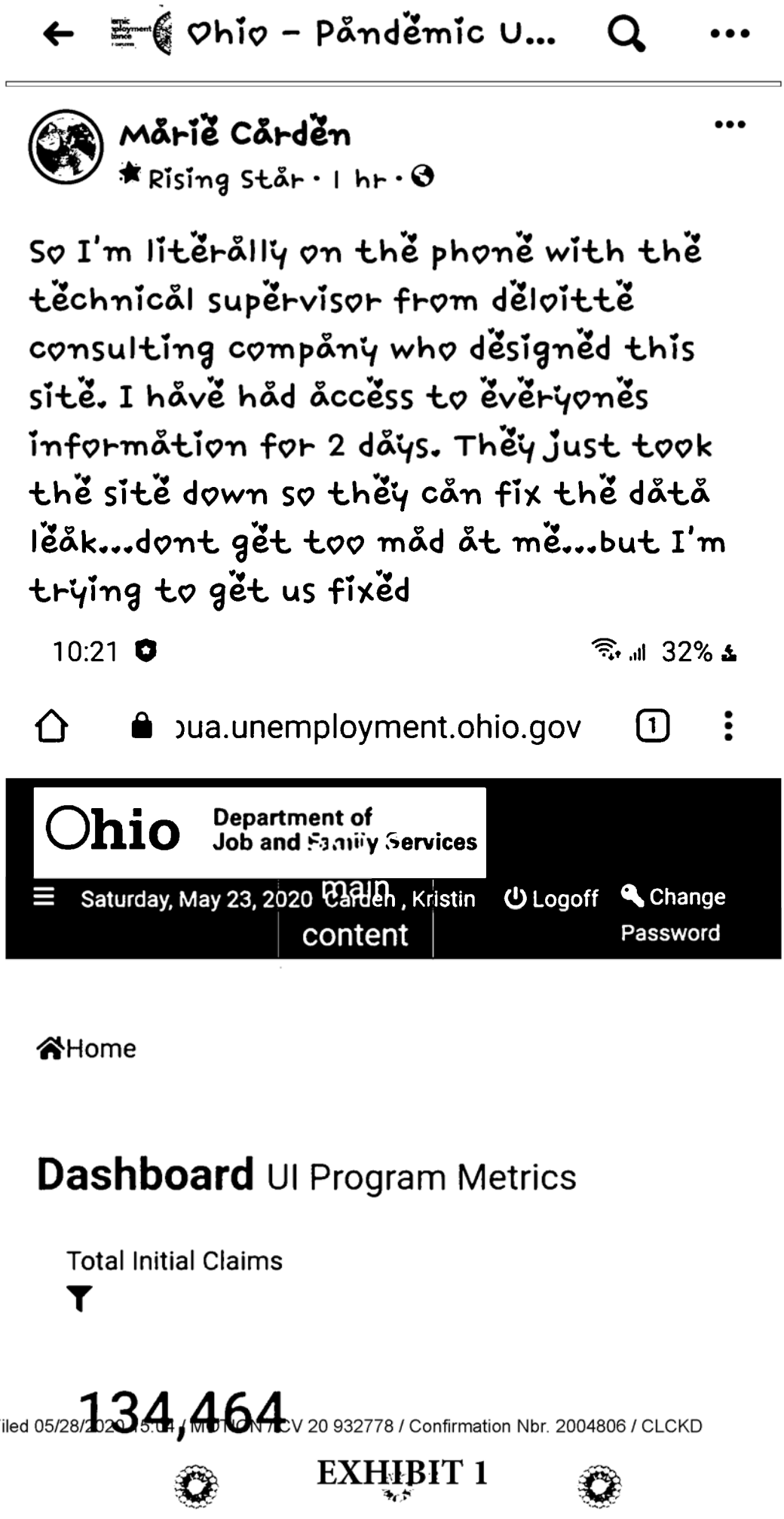


EXHIBIT 1

3:56 82%

Replies

Erica Dawn Miller

Yah the person threatened to leak my information so I'm reporting her got the screen shots as well

17m Like Reply 2

Sarah Latham

Erica Dawn Miller where'd she do that!? No cool!!!

11m Like Reply

Erica Dawn Miller

On a post in this group

8m Like Reply

Erica Dawn Miller

Sarah Latham

Write a reply... GIF

IN THE COURT OF COMMON PLEAS
CUYAHOGA COUNTY, OHIO

DANIEL BOZIN, individually and on behalf of all others similarly situated,
% DannLaw
PO Box 6031040
Cleveland, OH 44103

AND

TIMOTHY SMITH, individually and on behalf of all others similarly situated,
% DannLaw
PO Box 6031040
Cleveland, OH 44103

AND

ALEXANDRIA POLICHENA, individually and on behalf of all others similarly situated,
% DannLaw
PO Box 6031040
Cleveland, OH 44103

AND

BERNADETTE NOLEN, individually and on behalf of all others similarly situated,
% DannLaw
PO Box 6031040
Cleveland, OH 44103

AND

NICOLE HORNBECK, individually and on behalf of all others similarly situated,
% DannLaw
PO Box 6031040
Cleveland, OH 44103

Plaintiffs,

v.

Case No.: CV 20 932778

Judge David T. Matia

Electronically Filed 05/28/2020 15:04 / MOTION / CV 20 932778 / Confirmation Nbr. 2004806 / CLCKD

EXHIBIT C

DELOITTE CONSULTING LLP
% Corporation Service Company
50 West Broad Street, Suite 1330
Columbus, OH 43215

Defendant.

AFFIDAVIT OF BERNADETTE NOLEN IN SUPPORT OF PLAINTIFFS' EMERGNCY MOTION FOR A TEMPORARY RESTRAINING ORDER

I, BERNADETTE NOLEN, hereby certify as follows:

1. I am over the age of 18 years. I am competent and willing to testify as to the facts set forth in this Affidavit, which are based on my personal knowledge, unless stated otherwise.

2. I filed an application for Pandemic Unemployment Assistance ("PUA").

3. I received the Data Breach notice on or about May 20, 2020.

4. On May 22, 2020, I received PUA funds and they were directly deposited into my Netspend account, where I had requested the money be deposited.

5. On May 23, 2020, I received a text alert from Netspend stating that my card was reported stolen.

6. I had my card with me at the time I received the text alert from Netspend, and I had not reported it stolen.

7. I immediately called Netspend and the representative stated that my account was locked and my card had been canceled. I was told that a new card would be sent to me in one week, and I would be without access to much needed funds in the meantime.

8. A few hours later, I received an e-mail from Netspend notifying me of a transfer of a substantial amount of money from my supposedly locked account to another account. I had only one authorized account at the time—the account the money was transferred from—and I did

not authorize the transfer reported in the e-mail and did not own the account the money was being transferred to.

9. I immediately called Netspend to dispute the transfer, and I spent approximately an hour and a half on the phone with a Netspend representative attempting to understand what occurred, explain my predicament, and rectify the situation. During this phone call, I was told Netspend had three accounts in my name. The dispute is currently pending an internal investigation that could take months to resolve, according to Netspend.

10. In addition, I was notified that a substantial sum of money was wired by Western Union from my Netspend account. I immediately called a Western Union representative but was unable to get very far. The representative required a reference number to proceed that I did not have. I disputed the charge, and the dispute is currently pending Western Union's investigation.

11. On May 24, 2020, I again spoke with a Netspend representative and I was informed that an unauthorized person was attempting to order new cards associated with my Netspend account.

12. In addition, I was notified that my phone account was switched from my Boostmobile account to Metro using my personal and financial information. I did not authorize the switch. I now have a new phone, and the phone is not in my name for my protection.

13. I spent time and effort to file a police report relating to these events for my protection and to help to secure my information going forward. While the significant issues with my funds are being disputed, I am deprived of urgently needed money to provide for my children's basic needs, including healthcare, as well as my own.

I declare under penalty of perjury under laws of the State of Ohio that the foregoing statements are true and correct.

BERNADETTE NOLEN

County of Mahoning

State of Ohio

Sworn to and subscribed before me this 28th Day of May 2020

Notary Public

Kenneth C Kotouch
Notary Public
In and For the State of Ohio
My Commission Expires
04 August 2022

IN THE COURT OF COMMON PLEAS
CUYAHOGA COUNTY, OHIO

DANIEL BOZIN, individually and on behalf of all others similarly situated, *et al.* Plaintiffs, v. DELOITTE CONSULTING LLP Defendant.	Case No.: CV 20 932778 Judge David T. Matia

AFFIDAVIT OF MARC E. DANN IN SUPPORT OF PLAINTIFFS' EMERGENCY MOTION PURSUANT TO CIV. R. 65 FOR A TEMPORARY RESTRAINING ORDER AND/OR PRELIMINARY INJUNCTION

I, MARC E. DANN, hereby certify as follows:

1. I am over the age of 18 years. I am competent and willing to testify as to the facts set forth in this Affidavit, which are based on my personal knowledge, unless stated otherwise.

2. On May 22, 2020, I was contacted by Nicole Hornbeck regarding the underlying Complaint filed on May 20, 2020.

3. Ms. Hornbeck is now a co-Plaintiff in this action based on the First Amended Complaint filed on May 28, 2020.

4. On May 26, 2020, I sent Ms. Hornbeck a proposed affidavit which is attached hereto as **Exhibit 1**.

5. Ms. Hornbeck has confirmed with me that she will execute this affidavit but has been unable to secure a notary due to issues related to the COVID-19 pandemic.

6. We will supplement this affidavit and the injunction pleadings with the actual affidavits as soon as safe arrangements can be made for notarization.

EXHIBIT D

FURTHER SAYETH NAUGHT.

I affirm under the penalties of perjury that the above and foregoing statements and representations are true and correct.

Executed on this 28th day of May, 2020.

Marc E. Dann, Esq.

STATE OF OHIO

ss::

COUNTY OF Cuyahoga

Sworn to and subscribed before me, a notary public, this 28th day of May, 2020 by Marc E. Dann, the Affiant herein.

NOTARY PUBLIC
My Commission Expires: N/A

WILLIAM C. BEHRENS
ATTORNEY AT LAW
NOTARY PUBLIC
STATE OF OHIO
My Commission Has No Expiration Date
Sec 147.03 O.R.C.

IN THE COURT OF COMMON PLEAS
CUYAHOGA COUNTY, OHIO

DANIEL BOZIN, individually and on behalf of all others similarly situated,
% DannLaw
PO Box 6031040
Cleveland, OH 44103

AND

TIMOTHY SMITH, individually and on behalf of all others similarly situated,
% DannLaw
PO Box 6031040
Cleveland, OH 44103

AND

ALEXANDRIA POLICHENA, individually and on behalf of all others similarly situated,
% DannLaw
PO Box 6031040
Cleveland, OH 44103

AND

BERNADETTE NOLEN, individually and on behalf of all others similarly situated,
% DannLaw
PO Box 6031040
Cleveland, OH 44103

AND

NICOLE HORNBECK, individually and on behalf of all others similarly situated,
% DannLaw
PO Box 6031040
Cleveland, OH 44103

Plaintiffs,

v.

Case No.: CV 20 932778

Judge David T. Matia

Electronically Filed 05/28/2020 15:04 / MOTION / CV 20 932778 / Confirmation Nbr. 2004806 / CLCKD

EXHIBIT 1

DELOITTE CONSULTING LLP
% Corporation Service Company
50 West Broad Street, Suite 1330
Columbus, OH 43215

Defendant.

AFFIDAVIT OF NICOLE HORNBECK IN SUPPORT OF PLAINTIFFS' EMERGNCY MOTION FOR A TEMPORARY RESTRAINING ORDER

I, NICOLE HORNBECK, hereby certify as follows:

1. I am over the age of 18 years. I am competent and willing to testify as to the facts set forth in this Affidavit, which are based on my personal knowledge, unless stated otherwise.

2. On May 12, 2020, I filed an application for Pandemic Unemployment Assistance ("PUA"). I elected to receive my benefits by direct deposit to my Netspend bank account ("Account").

3. On May 20, 2020, I received an e-mail notifying me that my personal and financial information was exposed in the Data Breach.

4. On May 21, 2020, I received my PUA benefits, which were directly deposited in the Account.

5. Later that day, I received an alert from Netspend that my bank card linked to the Account was reported stolen. I knew it was not physically stolen, because I had it in my possession.

6. I immediately attempted to login to my bank account online, but my login credentials would not provide me access to my Account.

7. I called the bank, as I was concerned about the security of my Account. I provided my credentials and correctly answered the security questions, reset my credentials, and ordered a new bank card to be delivered to replace the now canceled card. I was without the use of the card until the canceled card would be replaced.

8. The next day, on May 22, 2020, I discovered that, using the updated account information, I was again locked out of my account.

9. In a follow up conversation with a Netspend representative, Netspend informed me that, after ten years of banking with Netspend, Netspend decided to end its banking relationship with me. Netspend informed me that it would send by mail a check for the money in my account that would reach me in 7–10 business days. Until I receive the check, I will not have access to the money in my account, which is the primary account for making purchases, and which includes the much-needed PUA benefits.

10. In addition, I received two alerts from my phone company, Boostmobile, that the pin on my account was requested. I had not requested the pin, nor authorized another person to do so. I made a phone call to Boostmobile to inquire, and to ensure the account was secure.

I declare under penalty of perjury under laws of the State of Ohio that the foregoing statements are true and correct.

_____

NICOLE HORNBECK

IN THE COURT OF COMMON PLEAS
CUYAHOGA COUNTY, OHIO

DANIEL BOZIN, individually and on behalf of all others similarly situated, *et al.* Plaintiffs, v. DELOITTE CONSULTING LLP Defendant.	Case No. CV-20-932778 Judge David T. Matia

TEMPORARY RESTRAINING ORDER

THIS MATTER coming on for hearing on Plaintiffs' Emergency Motion for a Temporary Restraining Order with notice, counsel for the Parties present, the Court being fully advised in the premises, with the Court hearing argument of counsel and the Court reviewing the pleadings, submissions and affidavits,

THE COURT FINDS:

(a) Plaintiffs have demonstrated a protectable interest and an ascertainable claim for relief with respect to their personal and financial information;

(b) Plaintiffs have demonstrated a showing of irreparable harm if this Court does not enter the Temporary Restraining Order to preserve the *status quo*;

(c) Plaintiffs have demonstrated that no adequate remedy at law exists, necessitating the entry of the Temporary Restraining Order;

(d) Plaintiffs have shown at least a fair question regarding the probability of success on the merits on the issues raised by the motion, which the Court finds are the issues predominating this proceeding;

(e) After reviewing the equities and balancing the hardships in entering the Temporary Restraining Order, the Court finds that the equities favor Plaintiffs;

(f) For good cause shown, the Court finds that the Temporary Restraining Order should be entered without a bond.

Electronically Filed 05/28/2020 15:04 / MOTION / CV 20 932778 / Confirmation Nbr. 2004806 / CLCKD

EXHIBIT E

IT IS HEREBY ORDERED:

1. Plaintiffs' Emergency Motion for a Temporary Restraining Order is granted.

2. Defendant is mandatorily enjoined to secure the personal and financial information of Plaintiffs and other Pandemic Unemployment Assistance applicants in Defendant's possession, custody, or control to prevent unauthorized access to it.

3. This injunction shall remain in full force and effect until _____.

4. This injunction is designed to maintain the *status quo* between the Parties.

5. This matter is set for status at _____ on _____, 2020, in Room _____, at which time a date will be set for a preliminary injunction hearing.

_____
Judge David T. Matia

Submitted by:

/s/ Marc Dann
Marc E. Dann (0039425)
Brian D. Flick (0081605)
DannLaw
P.O. Box 6031040
Cleveland, Ohio 44103
(216) 373-0539 telephone
(216) 373-0536 facsimile
notices@dannlaw.com

Thomas A. Zimmerman, Jr. (*pro hac vice* anticipated)
tom@attorneyzim.com
Zimmerman Law Offices, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
(312) 440-0020 telephone
(312) 440-4180 facsimile
www.attorneyzim.com

Counsel for Plaintiffs and the putative Class

Copies to:

Marc E. Dann, Esq., Brian D. Flick, Esq., Thomas A. Zimmerman, Jr., Esq., Counsel for the Plaintiffs and the putative Class
Daniel Warren, Esq., Counsel for Defendant